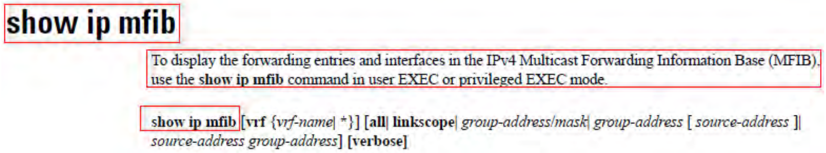
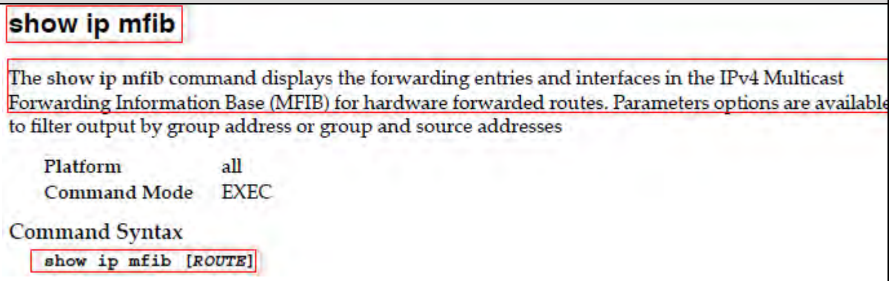
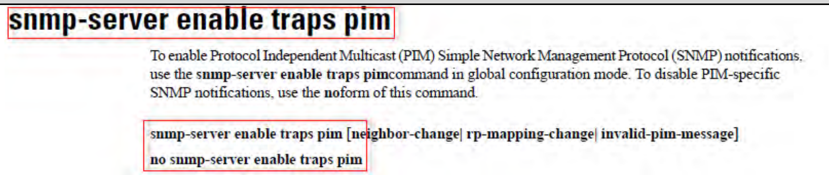
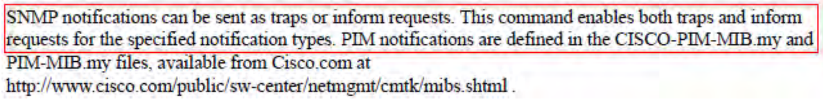
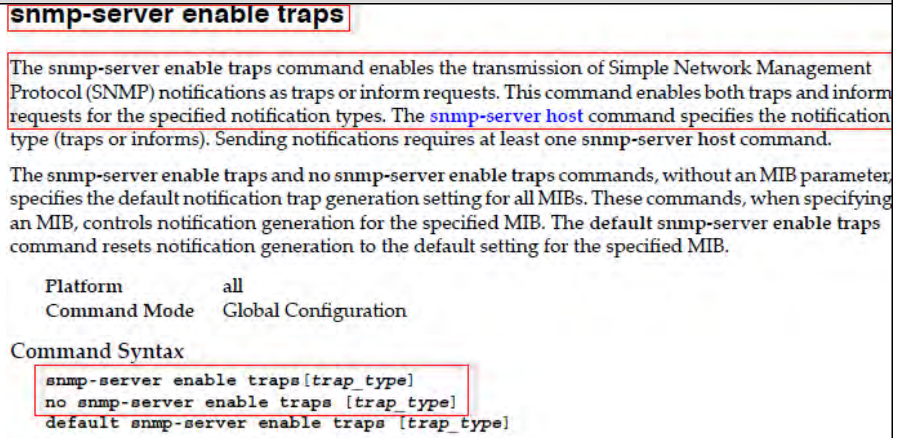
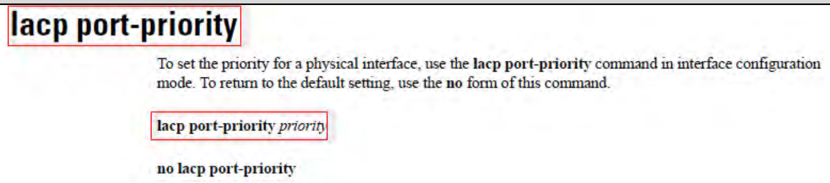
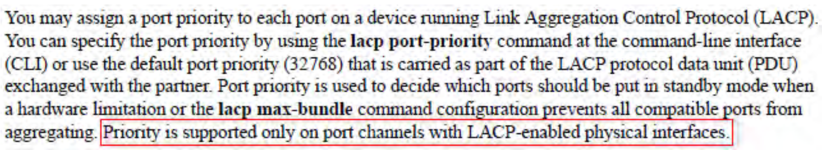
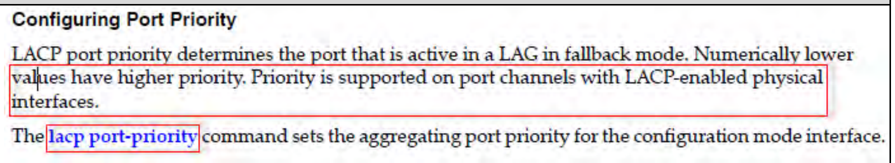
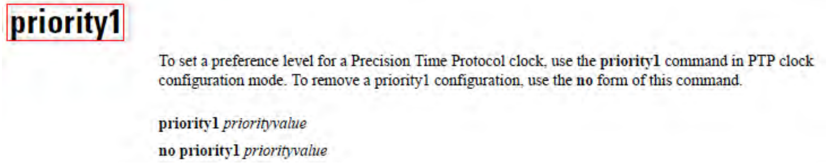
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **show ip mfib** To display the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB), use the **show ip mfib** command in user EXEC or privileged EXEC mode. **show ip mfib** [**vrf** {*vrf-name*| *}] [**all**| **linkscope**| *group-address/mask*| *group-address* [*source-address*]| *source-address group-address*] [**verbose**] Cisco IOS Multicast Command Reference (2013) at 649.	 **show ip mfib** The show ip mfib command displays the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB) for hardware forwarded routes. Parameters options are available to filter output by group address or group and source addresses Platform all Command Mode EXEC Command Syntax `show ip mfib [ROUTE]` Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1770 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1497; Arista User Manual, v. 4.11.1 (1/11/13), at 1196; Arista User Manual v. 4.10.3 (10/22/12), at 1020; Arista User Manual v. 4.9.3.2 (5/3/12), at 778; Arista User Manual v. 4.8.2 (11/18/11), at 597; Arista User Manual v. 4.7.3 (7/18/11), at 477; Arista User Manual v. 4.6.0 (12/22/2010), at 324.

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	
	snmp-server enable traps pim
	To enable Protocol Independent Multicast (PIM) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pim**command in global configuration mode. To disable PIM-specific SNMP notifications, use the **no**form of this command.
	snmp-server enable traps pim [neighbor-change| rp-mapping-change| invalid-pim-message]
	no snmp-server enable traps pim
	
	Cisco IOS Multicast Command Reference (2013), at 950.
	
	
	SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files, available from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .
	
	Cisco IOS Multicast Command Reference (2013), at 951.
		
		snmp-server enable traps
		The **snmp-server enable traps** command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The snmp-server host command specifies the notification type (traps or informs). Sending notifications requires at least one **snmp-server host** command.
		The **snmp-server enable traps** and **no snmp-server enable traps** commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The **default snmp-server enable traps** command resets notification generation to the default setting for the specified MIB.
		Platform all
		Command Mode Global Configuration
		Command Syntax
		`snmp-server enable traps[trap_type]`
		`no snmp-server enable traps [trap_type]`
		`default snmp-server enable traps [trap_type]`
		
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1990.
		
		See also Arista User Manual v. 4.13.6F (4/14/2014), at 1918; Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **lacp port-priority** To set the priority for a physical interface, use the **lacp port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command. **lacp port-priority** *priority* **no lacp port-priority** Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 690.  You may assign a port priority to each port on a device running Link Aggregation Control Protocol (LACP). You can specify the port priority by using the **lacp port-priority** command at the command-line interface (CLI) or use the default port priority (32768) that is carried as part of the LACP protocol data unit (PDU) exchanged with the partner. Port priority is used to decide which ports should be put in standby mode when a hardware limitation or the **lacp max-bundle** command configuration prevents all compatible ports from aggregating. Priority is supported only on port channels with LACP-enabled physical interfaces. Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 691.	 **Configuring Port Priority** LACP port priority determines the port that is active in a LAG in fallback mode. Numerically lower values have higher priority. Priority is supported on port channels with LACP-enabled physical interfaces. The lacp port-priority command sets the aggregating port priority for the configuration mode interface. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 461. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 395; Arista User Manual, v. 4.11.1 (1/11/13), at 333; Arista User Manual v. 4.10.3 (10/22/12), at 291; Arista User Manual v. 4.9.3.2 (5/3/12), at 275; Arista User Manual v. 4.8.2 (11/18/11), at 207.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>


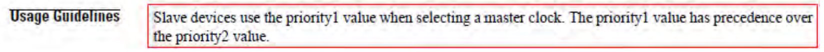
<b>priority1</b>

To set a preference level for a Precision Time Protocol clock, use the <b>priority1</b> command in PTP clock configuration mode. To remove a priority1 configuration, use the <b>no</b> form of this command.

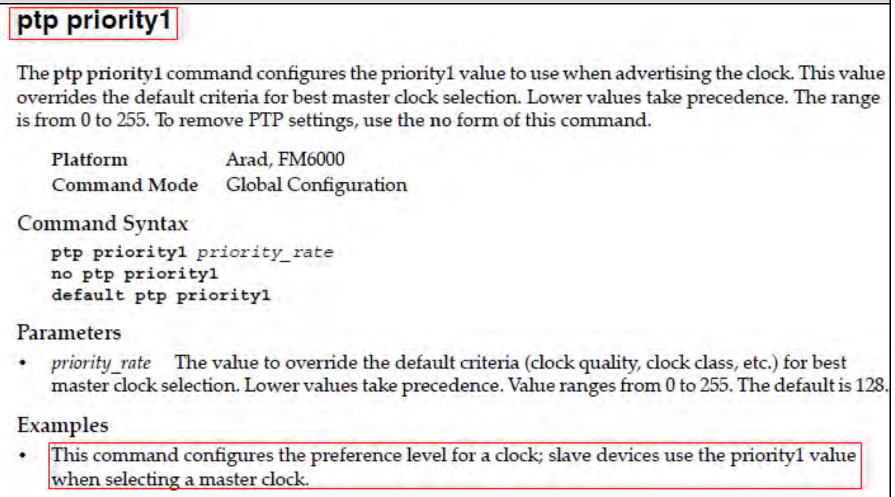
<b>priority1</b> <i>priorityvalue</i>

<b>no priority1</b> <i>priorityvalue</i>

. . .



<b>Usage Guidelines</b> Slave devices use the priority1 value when selecting a master clock. The priority1 value has precedence over the priority2 value.

Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 1003.
</td>
<td>


<b>ptp priority1</b>

The ptp priority1 command configures the priority1 value to use when advertising the clock. This value overrides the default criteria for best master clock selection. Lower values take precedence. The range is from 0 to 255. To remove PTP settings, use the no form of this command.

Platform Arad, FM6000
Command Mode Global Configuration

Command Syntax

<code>ptp priority1 <i>priority_rate</i></code>
<code>no ptp priority1</code>
<code>default ptp priority1</code>

Parameters

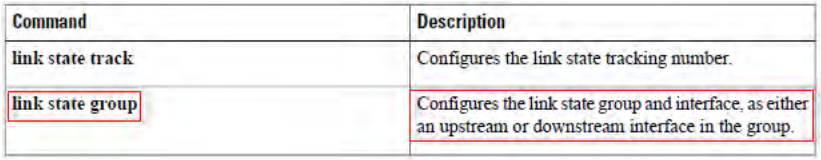
- <i>priority_rate</i> The value to override the default criteria (clock quality, clock class, etc.) for best master clock selection. Lower values take precedence. Value ranges from 0 to 255. The default is 128.

Examples

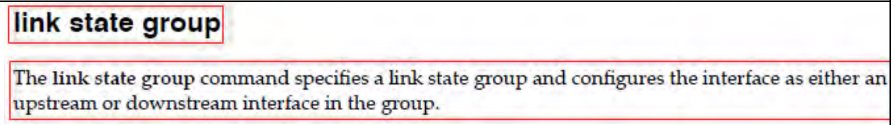
- This command configures the preference level for a clock; slave devices use the priority1 value when selecting a master clock.

Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 326.

<i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 318; Arista User Manual v. 4.12.3 (7/17/13), at 262; Arista User Manual, v. 4.11.1 (1/11/13), at 208.
</td>
</tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>


<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>link state track</td><td>Configures the link state tracking number.</td></tr>
<tr><td>link state group</td><td>Configures the link state group and interface, as either an upstream or downstream interface in the group.</td></tr>
</table>

Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 1950.
</td>
<td>


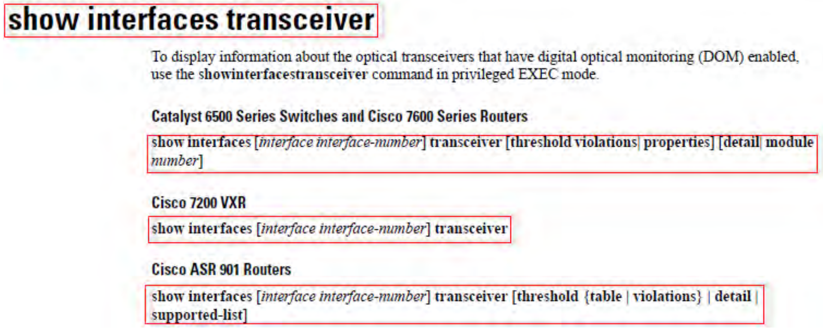
<b>link state group</b>

The link state group command specifies a link state group and configures the interface as either an upstream or downstream interface in the group.

Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 659.

<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 527; Arista User Manual, v. 4.11.1 (1/11/13), at 422.
</td>
</tr>
</table>

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td></td>
<td>



show interfaces transceiver

To display information about the optical transceivers that have digital optical monitoring (DOM) enabled, use the showinterfacestransceiver command in privileged EXEC mode.

Catalyst 6500 Series Switches and Cisco 7600 Series Routers

show interfaces [*interface interface-number*] **transceiver** [**threshold violations**| **properties**] [**detail**| **module** *number*]

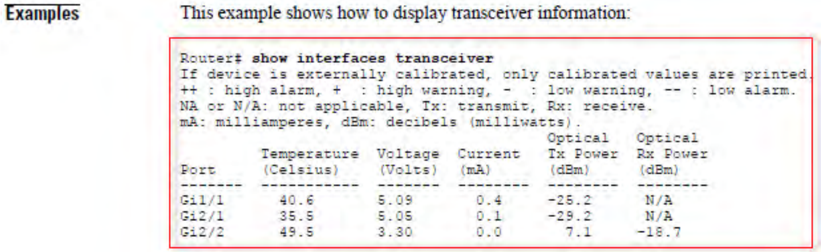
Cisco 7200 VXR

show interfaces [*interface interface-number*] **transceiver**

Cisco ASR 901 Routers

show interfaces [*interface interface-number*] **transceiver** [**threshold** {**table** | **violations**} | **detail** | **supported-list**]

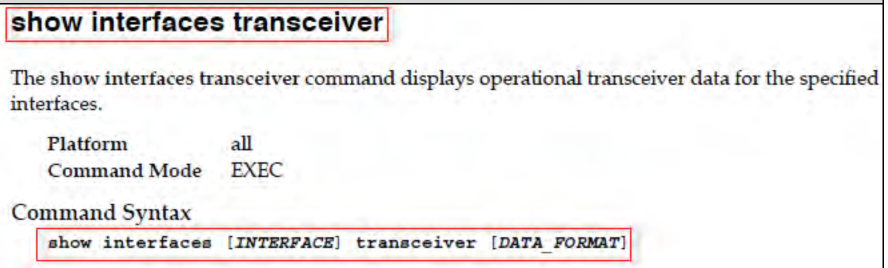
Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 1878.



Examples This example shows how to display transceiver information:

```
Router# show interfaces transceiver
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
                                            Optical   Optical
         Temperature  Voltage  Current     Tx Power  Rx Power
Port     (Celsius)    (Volts)  (mA)        (dBm)     (dBm)
-------  -----------  -------  --------    --------  --------
Gi1/1      40.6       5.09       0.4       -25.2      N/A
Gi2/1      35.5       5.05       0.1       -29.2      N/A
Gi2/2      49.5       3.30       0.0         7.1     -18.7
```

</td>
<td>



show interfaces transceiver

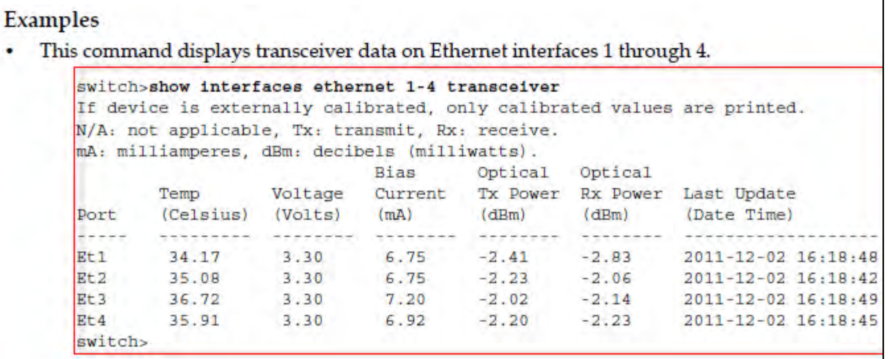
The show interfaces transceiver command displays operational transceiver data for the specified interfaces.

Platform all
Command Mode EXEC

Command Syntax

```
show interfaces [INTERFACE] transceiver [DATA_FORMAT]
```

. . .



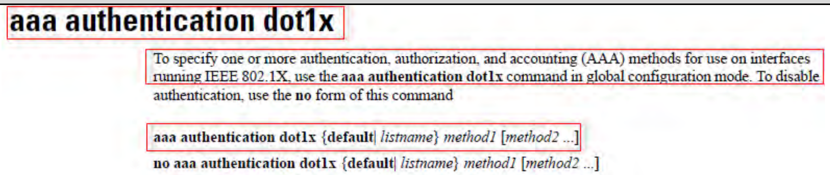
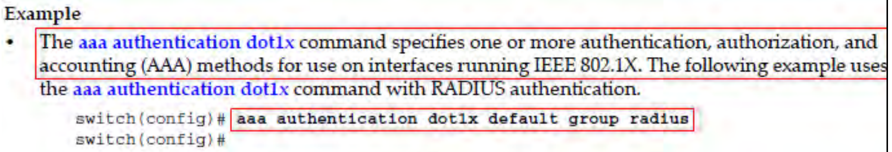
Examples

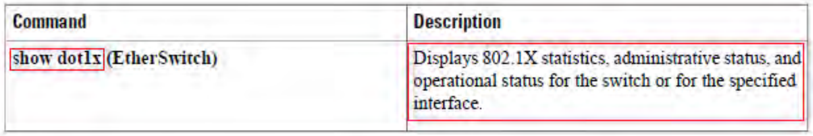
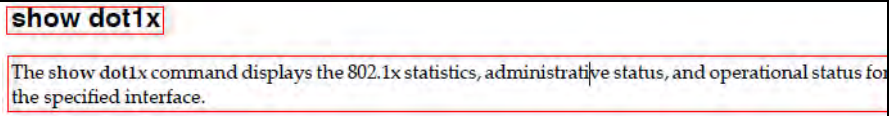
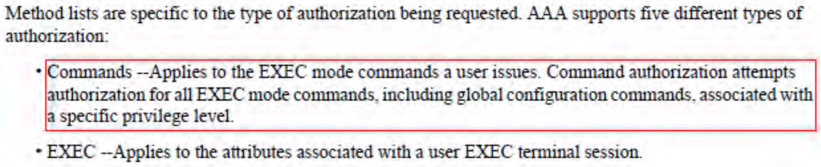
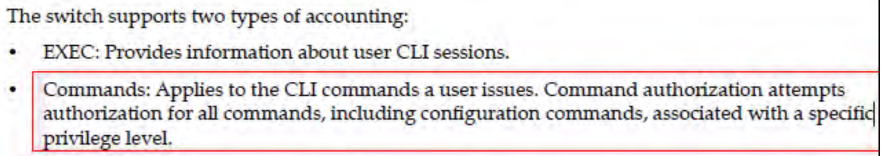
- This command displays transceiver data on Ethernet interfaces 1 through 4.

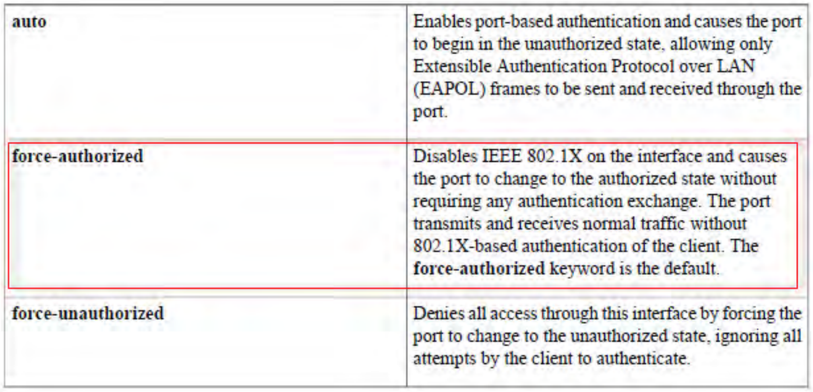
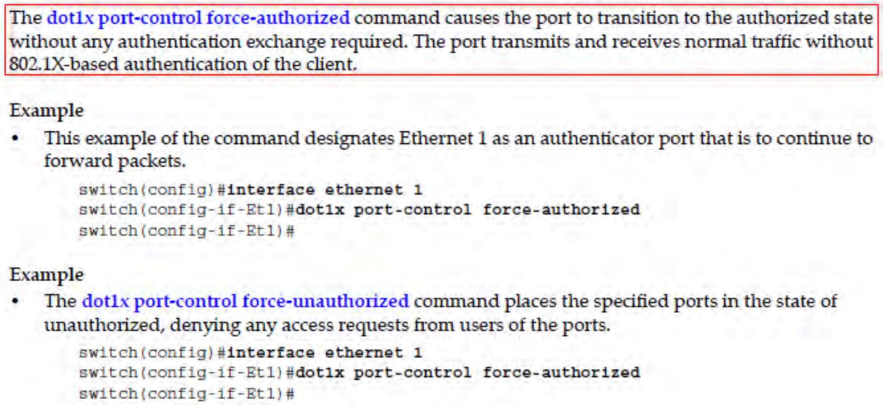
```
switch>show interfaces ethernet 1-4 transceiver
If device is externally calibrated, only calibrated values are printed.
N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
                                 Bias      Optical   Optical
        Temp       Voltage   Current   Tx Power  Rx Power  Last Update
Port    (Celsius)  (Volts)   (mA)      (dBm)     (dBm)     (Date Time)
-----   ---------  --------  --------  --------  --------  -------------------
Et1      34.17      3.30      6.75     -2.41     -2.83     2011-12-02 16:18:48
Et2      35.08      3.30      6.75     -2.23     -2.06     2011-12-02 16:18:42
Et3      36.72      3.30      7.20     -2.02     -2.14     2011-12-02 16:18:49
Et4      35.91      3.30      6.92     -2.20     -2.23     2011-12-02 16:18:45
switch>
```

</td>
</tr>
<tr>
<td>Cisco IOS 15.4
Effective date of registration: 11/26/2014</td>
<td>Cisco IOS Interfaces and Hardware Component Command Reference (2013), at 1879.</td>
<td>Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 451.
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 385; Arista User Manual, v. 4.11.1 (1/11/13), at 326; Arista User Manual v. 4.10.3 (10/22/12), at 284; Arista User Manual v. 4.9.3.2 (5/3/12), at 266.</td>
</tr>
</table>

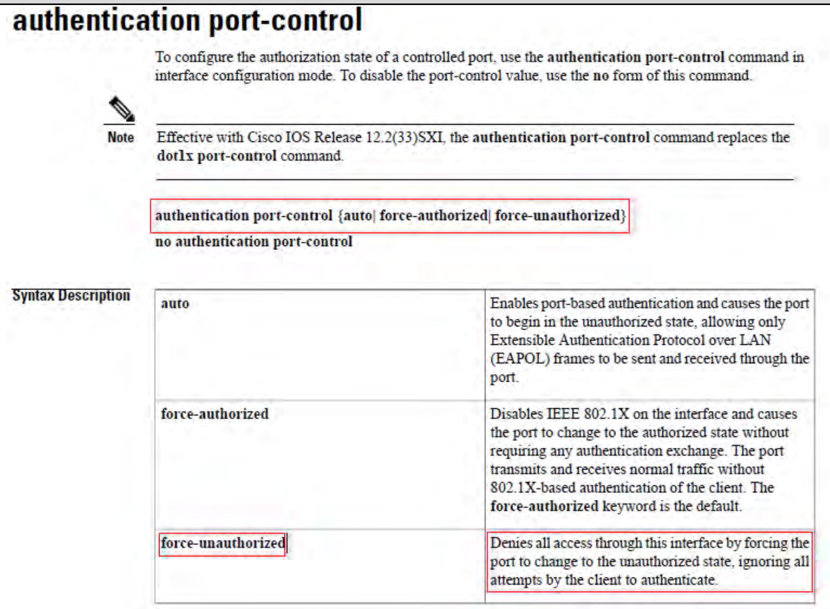
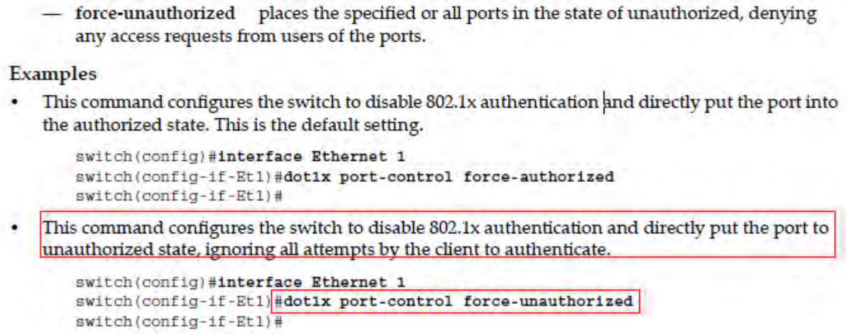
Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	aaa authentication dot1x
	To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command
	aaa authentication dot1x {**default**| *listname*} *method1* [*method2* ...]
	no aaa authentication dot1x {**default**| *listname*} *method1* [*method2* ...]
	Cisco IOS Security Command Reference: Commands A to C (2013), at 54.
		
		Example
		• The aaa authentication dot1x command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X. The following example uses the aaa authentication dot1x command with RADIUS authentication.
		`switch(config)# aaa authentication dot1x default group radius`
		`switch(config)#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 557.

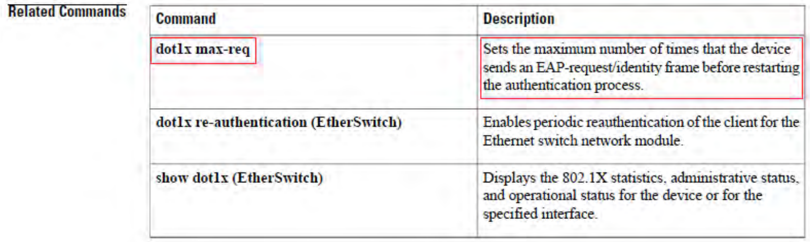
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Command**: **show dot1x** (**EtherSwitch**) **Description**: Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface. Cisco IOS Security Command Reference: Commands A to C (2013), at 56.	 **show dot1x** The show dot1x command displays the 802.1x statistics, administrative status, and operational status for the specified interface. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 572.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization: • Commands --Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level. • EXEC --Applies to the attributes associated with a user EXEC terminal session. Cisco IOS Security Command Reference: Commands A to C (2013), at 83.	 The switch supports two types of accounting: • EXEC: Provides information about user CLI sessions. • Commands: Applies to the CLI commands a user issues. Command authorization attempts authorization for all commands, including configuration commands, associated with a specific privilege level. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 207. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 154; Arista User Manual, v. 4.11.1 (1/11/13), at 114; Arista User Manual v. 4.10.3 (10/22/12), at 106; Arista User Manual v. 4.9.3.2 (5/3/12), at 93; Arista User Manual v. 4.8.2 (11/18/11), at 87; Arista User Manual v. 4.7.3 (7/18/11), at 73.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **auto** — Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port. **force-authorized** — Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default. **force-unauthorized** — Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate. Cisco IOS Security Command Reference: Commands A to C (2013), at 354.	 The dot1x port-control force-authorized command causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. **Example** - This example of the command designates Ethernet 1 as an authenticator port that is to continue to forward packets. `switch(config)#`**`interface ethernet 1`** `switch(config-if-Et1)#`**`dot1x port-control force-authorized`** `switch(config-if-Et1)#` **Example** - The dot1x port-control force-unauthorized command places the specified ports in the state of unauthorized, denying any access requests from users of the ports. `switch(config)#`**`interface ethernet 1`** `switch(config-if-Et1)#`**`dot1x port-control force-authorized`** `switch(config-if-Et1)#` Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 558.

Copyright Registration Information	Cisco	Arista

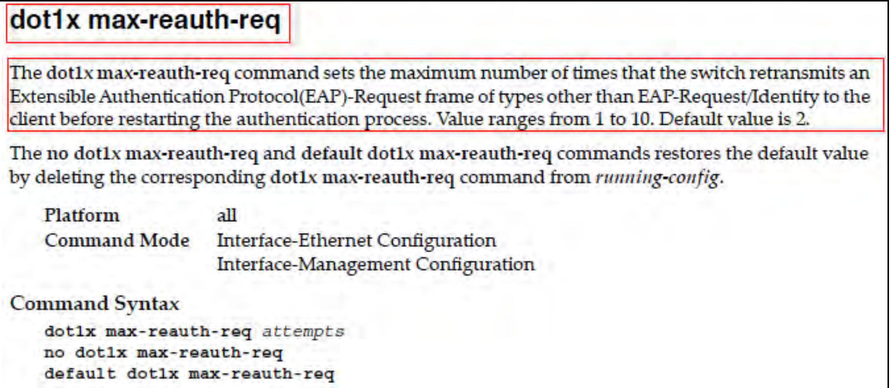
Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	authentication port-control
	To configure the authorization state of a controlled port, use the **authentication port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.
	Note Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1x port-control** command.
	authentication port-control {**auto**| **force-authorized**| **force-unauthorized**}
	no authentication port-control
	Syntax Description
	auto
	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
	force-authorized
	Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
	force-unauthorized
	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.
	Cisco IOS Security Command Reference: Commands A to C (2013), at 354.
		
		— **force-unauthorized** places the specified or all ports in the state of unauthorized, denying any access requests from users of the ports.
		Examples
		• This command configures the switch to disable 802.1x authentication and directly put the port into the authorized state. This is the default setting.
		`switch(config)#interface Ethernet 1`
		`switch(config-if-Et1)#dot1x port-control force-authorized`
		`switch(config-if-Et1)#`
		• This command configures the switch to disable 802.1x authentication and directly put the port to unauthorized state, ignoring all attempts by the client to authenticate.
		`switch(config)#interface Ethernet 1`
		`switch(config-if-Et1)#dot1x port-control force-unauthorized`
		`switch(config-if-Et1)#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 567.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>


Related Commands

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>dot1x max-req</b></td><td>Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.</td></tr>
<tr><td><b>dot1x re-authentication (EtherSwitch)</b></td><td>Enables periodic reauthentication of the client for the Ethernet switch network module.</td></tr>
<tr><td><b>show dot1x (EtherSwitch)</b></td><td>Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.</td></tr>
</table>

Cisco IOS Security Command Reference: Commands D to L (2013), at 219.
</td>
<td>


<b>dot1x max-reauth-req</b>

The <b>dot1x max-reauth-req</b> command sets the maximum number of times that the switch retransmits an Extensible Authentication Protocol(EAP)-Request frame of types other than EAP-Request/Identity to the client before restarting the authentication process. Value ranges from 1 to 10. Default value is 2.

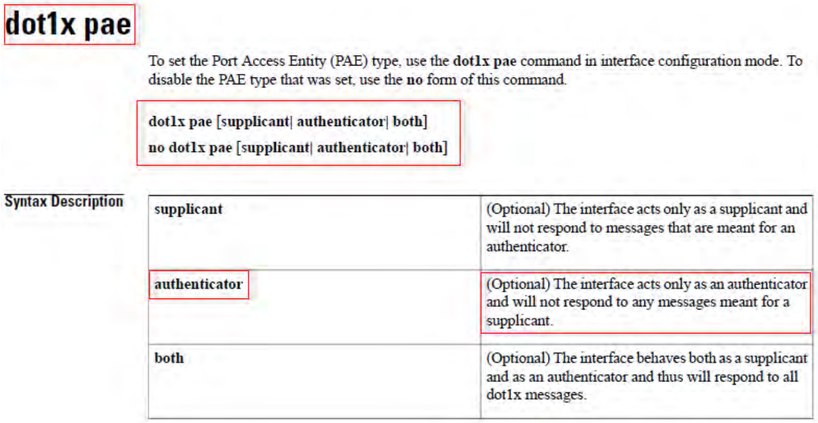
The <b>no dot1x max-reauth-req</b> and <b>default dot1x max-reauth-req</b> commands restores the default value by deleting the corresponding <b>dot1x max-reauth-req</b> command from <i>running-config</i>.

Platform all
Command Mode Interface-Ethernet Configuration
Interface-Management Configuration

Command Syntax

```
dot1x max-reauth-req attempts
no dot1x max-reauth-req
default dot1x max-reauth-req
```

Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 565.
</td>
</tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>


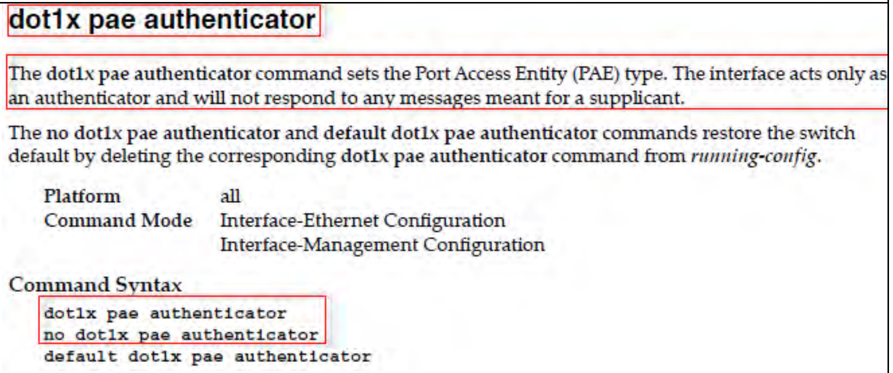
<b>dot1x pae</b>

To set the Port Access Entity (PAE) type, use the <b>dot1x pae</b> command in interface configuration mode. To disable the PAE type that was set, use the <b>no</b> form of this command.

<b>dot1x pae [supplicant| authenticator| both]</b>
<b>no dot1x pae [supplicant| authenticator| both]</b>

Syntax Description

<table>
<tr><td><b>supplicant</b></td><td>(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.</td></tr>
<tr><td><b>authenticator</b></td><td>(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.</td></tr>
<tr><td><b>both</b></td><td>(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.</td></tr>
</table>

Cisco IOS Security Command Reference: Commands D to L (2013), at 195.
</td>
<td>


<b>dot1x pae authenticator</b>

The <b>dot1x pae authenticator</b> command sets the Port Access Entity (PAE) type. The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.

The <b>no dot1x pae authenticator</b> and <b>default dot1x pae authenticator</b> commands restore the switch default by deleting the corresponding <b>dot1x pae authenticator</b> command from <i>running-config</i>.

Platform all
Command Mode Interface-Ethernet Configuration
Interface-Management Configuration

Command Syntax

```
dot1x pae authenticator
no dot1x pae authenticator
default dot1x pae authenticator
```

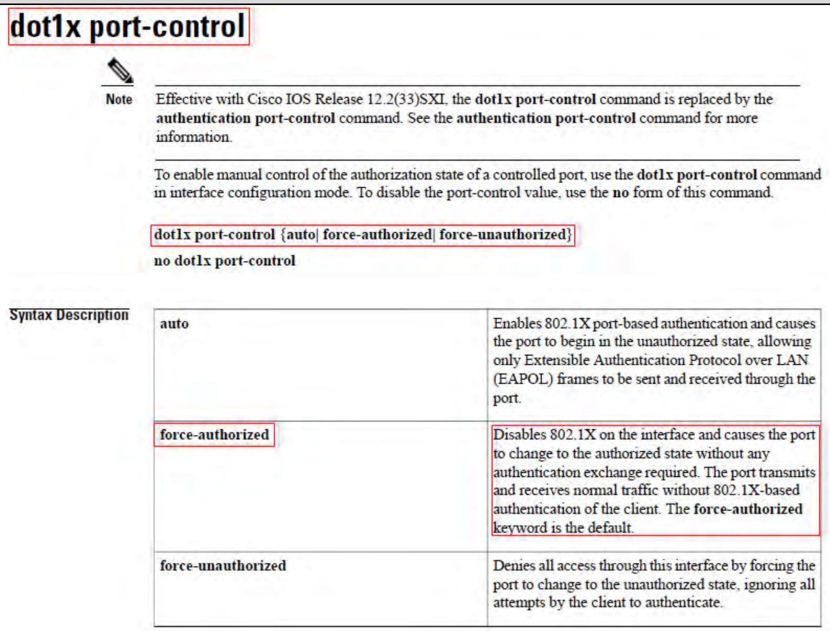
Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 567.
</td>
</tr>
</table>

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>

Cisco IOS 15.4

Effective date of registration: 11/26/2014

</td>
<td>



dot1x port-control

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x port-control** command is replaced by the **authentication port-control** command. See the **authentication port-control** command for more information.

To enable manual control of the authorization state of a controlled port, use the **dot1x port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

dot1x port-control {**auto**| **force-authorized**| **force-unauthorized**}

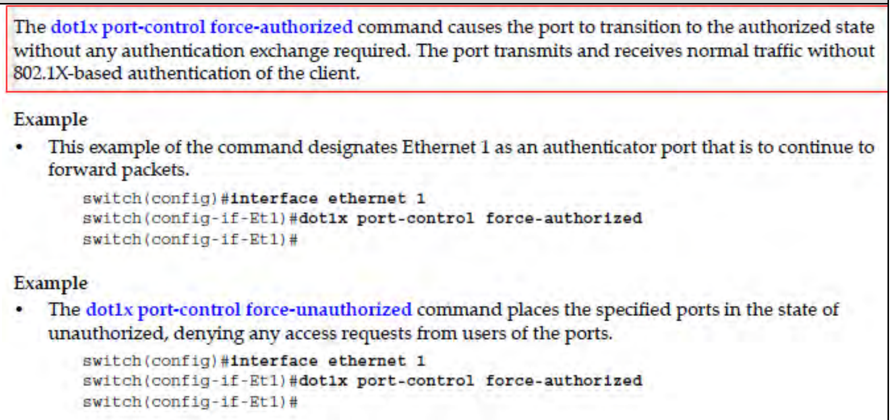
no dot1x port-control

Syntax Description

auto	Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Cisco IOS Security Command Reference: Commands D to L (2013), at 197.

</td>
<td>



The dot1x port-control force-authorized command causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.

Example

- This example of the command designates Ethernet 1 as an authenticator port that is to continue to forward packets.

```
switch(config)#interface ethernet 1
switch(config-if-Et1)#dot1x port-control force-authorized
switch(config-if-Et1)#
```

Example

- The dot1x port-control force-unauthorized command places the specified ports in the state of unauthorized, denying any access requests from users of the ports.

```
switch(config)#interface ethernet 1
switch(config-if-Et1)#dot1x port-control force-authorized
switch(config-if-Et1)#
```

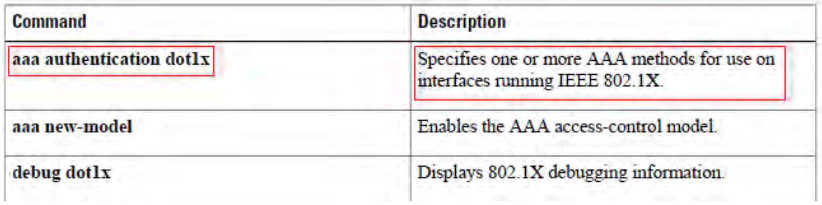
Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 558.

</td>
</tr>
<tr>
<td>

Cisco IOS 15.4

Effective date of registration: 11/26/2014

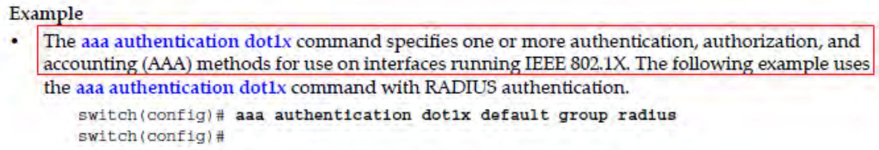
</td>
<td>



Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa new-model	Enables the AAA access-control model.
debug dot1x	Displays 802.1X debugging information.

Cisco IOS Security Command Reference: Commands D to L (2013), at 211.

</td>
<td>



Example

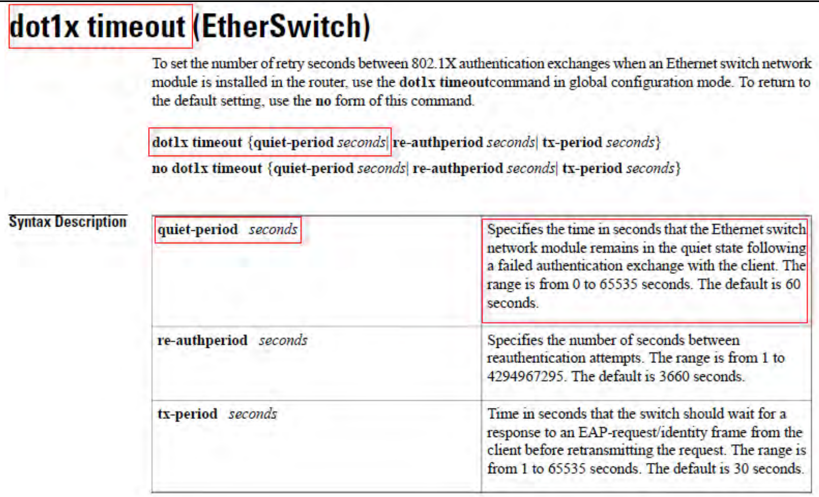
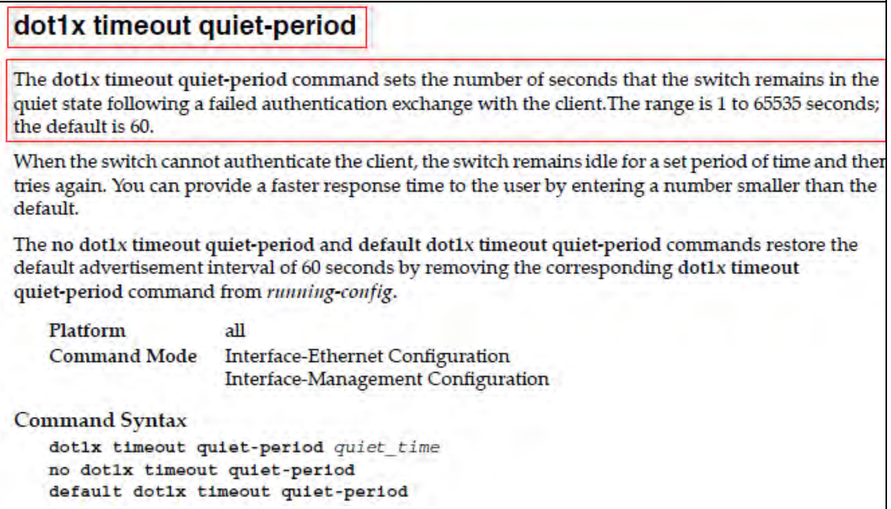
- The aaa authentication dot1x command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X. The following example uses the aaa authentication dot1x command with RADIUS authentication.

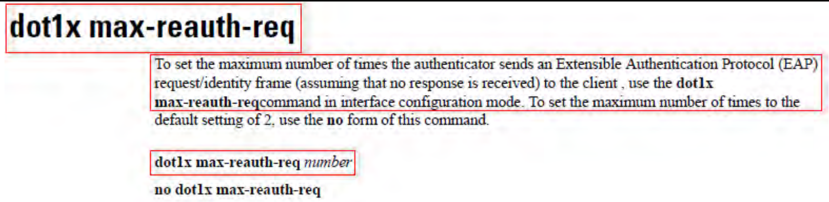
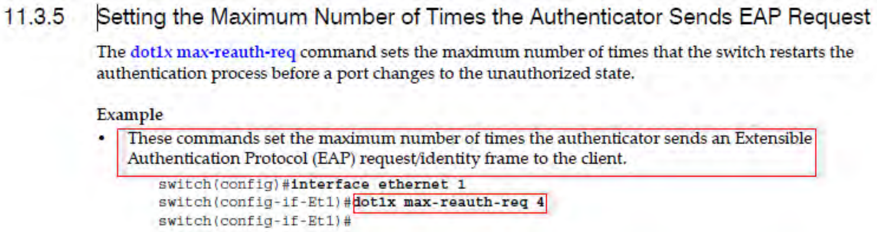
```
switch(config)# aaa authentication dot1x default group radius
switch(config)#
```

Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 557.

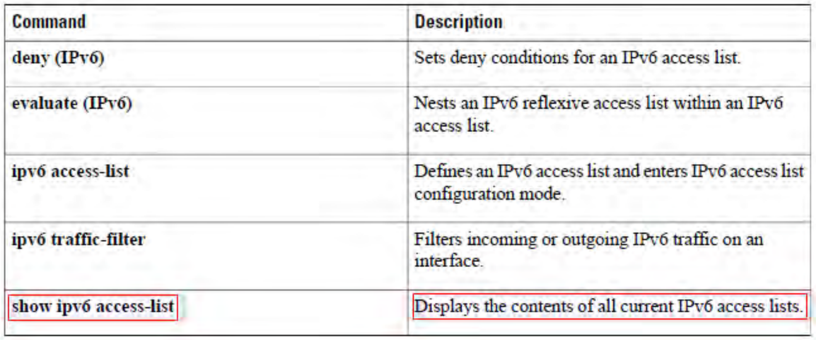
</td>
</tr>
</table>

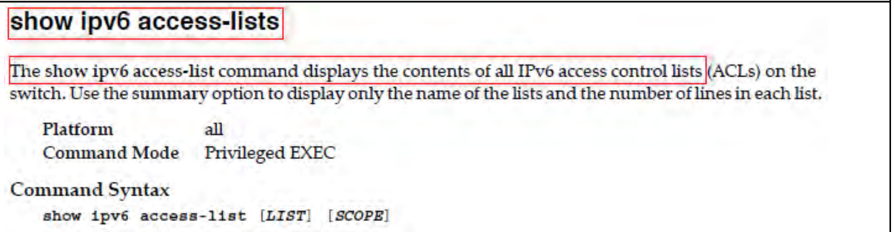
Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	dot1x timeout (EtherSwitch)
	To set the number of retry seconds between 802.1X authentication exchanges when an Ethernet switch network module is installed in the router, use the **dot1x timeout**command in global configuration mode. To return to the default setting, use the **no** form of this command.
	dot1x timeout {**quiet-period** *seconds*| **re-authperiod** *seconds*| **tx-period** *seconds*}
	no dot1x timeout {**quiet-period** *seconds*| **re-authperiod** *seconds*| **tx-period** *seconds*}
	Syntax Description
	quiet-period *seconds* — Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds.
	re-authperiod *seconds* — Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3660 seconds.
	tx-period *seconds* — Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is from 1 to 65535 seconds. The default is 30 seconds.
	Cisco IOS Security Command Reference: Commands D to L (2013), at 218.
		
		dot1x timeout quiet-period
		The **dot1x timeout quiet-period** command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.The range is 1 to 65535 seconds; the default is 60.
		When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default.
		The **no dot1x timeout quiet-period** and **default dot1x timeout quiet-period** commands restore the default advertisement interval of 60 seconds by removing the corresponding **dot1x timeout quiet-period** command from *running-config*.
		Platform all
		Command Mode Interface-Ethernet Configuration
		Interface-Management Configuration
		Command Syntax
		`dot1x timeout quiet-period quiet_time`
		`no dot1x timeout quiet-period`
		`default dot1x timeout quiet-period`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 569.

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	dot1x max-reauth-req
	To set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client , use the **dot1x max-reauth-req**command in interface configuration mode. To set the maximum number of times to the default setting of 2, use the **no** form of this command.
	dot1x max-reauth-req *number*
	no dot1x max-reauth-req
	Cisco IOS Security Command Reference: Commands D to L (2013), at 185.
		
		11.3.5 Setting the Maximum Number of Times the Authenticator Sends EAP Request
		The dot1x max-reauth-req command sets the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state.
		Example
		• These commands set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame to the client.
		`switch(config)#interface ethernet 1`
		`switch(config-if-Et1)#dot1x max-reauth-req 4`
		`switch(config-if-Et1)#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 559.

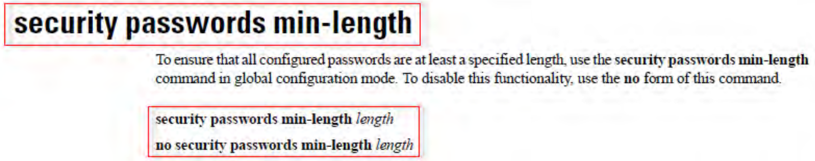
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>deny (IPv6)</b></td><td>Sets deny conditions for an IPv6 access list.</td></tr>
<tr><td><b>evaluate (IPv6)</b></td><td>Nests an IPv6 reflexive access list within an IPv6 access list.</td></tr>
<tr><td><b>ipv6 access-list</b></td><td>Defines an IPv6 access list and enters IPv6 access list configuration mode.</td></tr>
<tr><td><b>ipv6 traffic-filter</b></td><td>Filters incoming or outgoing IPv6 traffic on an interface.</td></tr>
<tr><td><b>show ipv6 access-list</b></td><td>Displays the contents of all current IPv6 access lists.</td></tr>
</table>

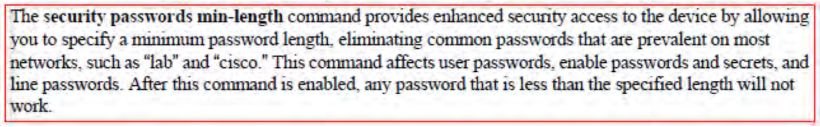
Cisco IOS Security Command Reference: Commands M to R at 440 (2013).
</td>
<td>

<b>show ipv6 access-lists</b>
The show ipv6 access-list command displays the contents of all IPv6 access control lists (ACLs) on the switch. Use the summary option to display only the name of the lists and the number of lines in each list.
Platform all
Command Mode Privileged EXEC
Command Syntax
<code>show ipv6 access-list [LIST] [SCOPE]</code>

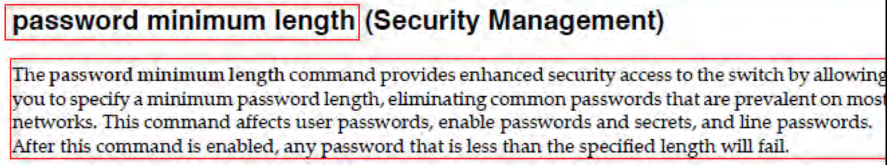
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 904.

<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 782; Arista User Manual, v. 4.11.1 (1/11/13), at 611; Arista User Manual v. 4.10.3 (10/22/12), at 525.
</td>
</tr>
<tr>
<td>Cisco IOS 15.4

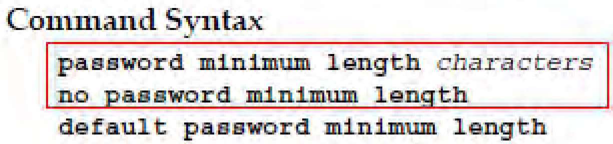
Effective date of registration: 11/26/2014</td>
<td>

<b>security passwords min-length</b>
To ensure that all configured passwords are at least a specified length, use the <b>security passwords min-length</b> command in global configuration mode. To disable this functionality, use the <b>no</b> form of this command.
<b>security passwords min-length</b> <i>length</i>
<b>no security passwords min-length</b> <i>length</i>

. . .

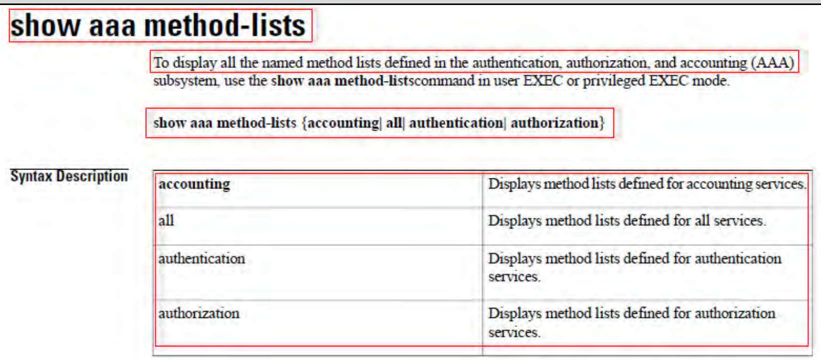
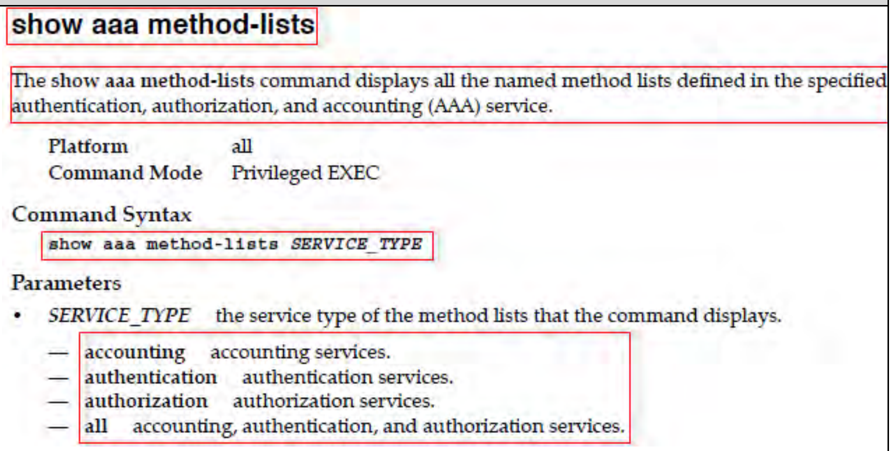
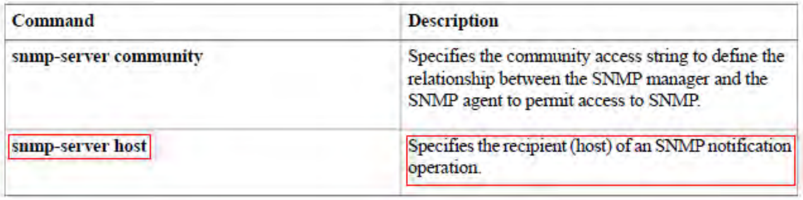
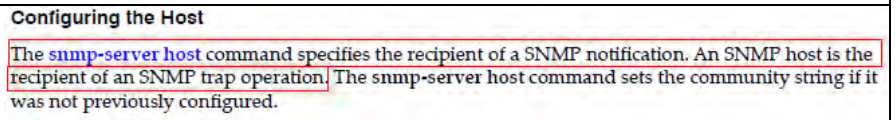

The <b>security passwords min-length</b> command provides enhanced security access to the device by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as “lab” and “cisco.” This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will not work.

Cisco IOS Security Command Reference: Commands S to Z at 37 (2013).
</td>
<td>

<b>password minimum length (Security Management)</b>
The password minimum length command provides enhanced security access to the switch by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks. This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail.

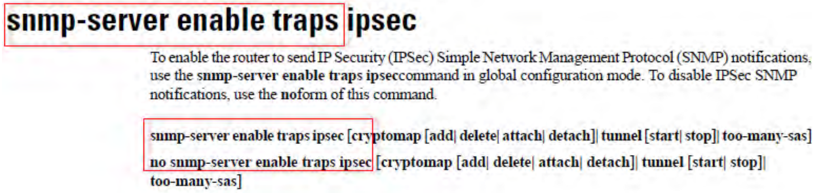
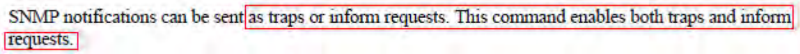
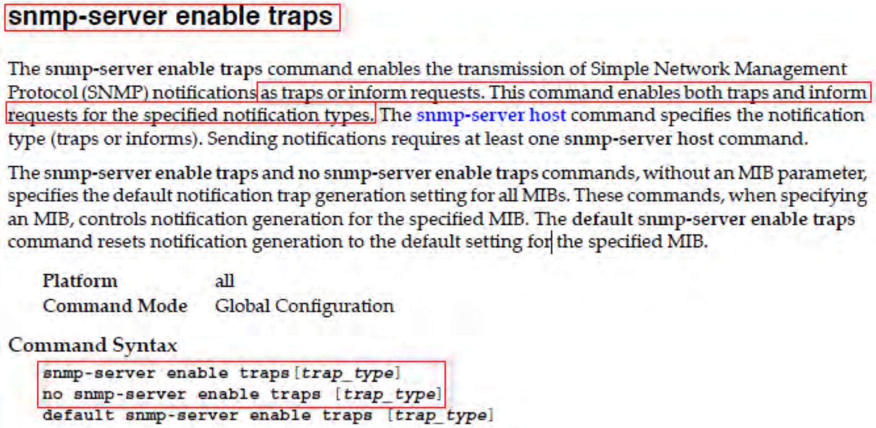
. . .


Command Syntax
<code>password minimum length <i>characters</i></code>
<code>no password minimum length</code>
<code>default password minimum length</code>

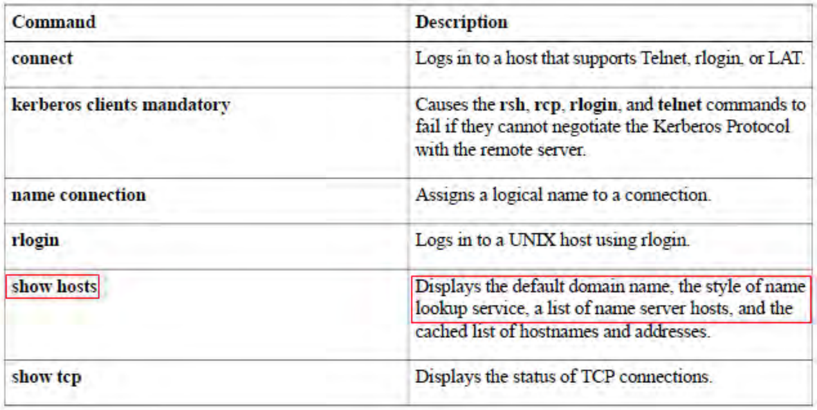
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 158.
</td>
</tr>
</table>

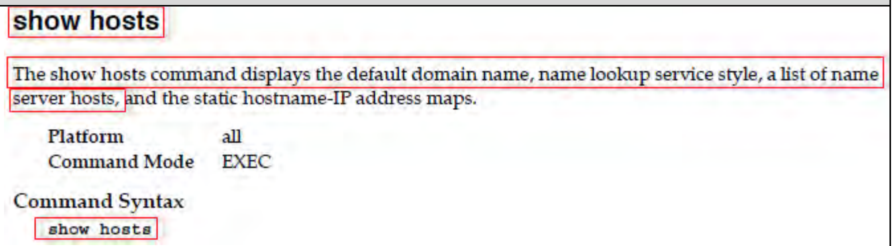
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4
Effective date of registration: 11/26/2014</td>
<td>

<b>show aaa method-lists</b>
To display all the named method lists defined in the authentication, authorization, and accounting (AAA) subsystem, use the <b>show aaa method-lists</b>command in user EXEC or privileged EXEC mode.
<b>show aaa method-lists</b> {<b>accounting</b>| <b>all</b>| <b>authentication</b>| <b>authorization</b>}
Syntax Description
<table>
<tr><td><b>accounting</b></td><td>Displays method lists defined for accounting services.</td></tr>
<tr><td>all</td><td>Displays method lists defined for all services.</td></tr>
<tr><td>authentication</td><td>Displays method lists defined for authentication services.</td></tr>
<tr><td>authorization</td><td>Displays method lists defined for authorization services.</td></tr>
</table>
Cisco IOS Security Command Reference: Commands S to Z at 185 (2013).
</td>
<td>

<b>show aaa method-lists</b>
The <b>show aaa method-lists</b> command displays all the named method lists defined in the specified authentication, authorization, and accounting (AAA) service.
Platform all
Command Mode Privileged EXEC
Command Syntax
<code>show aaa method-lists <i>SERVICE_TYPE</i></code>
Parameters
• <i>SERVICE_TYPE</i> the service type of the method lists that the command displays.
— <b>accounting</b> accounting services.
— <b>authentication</b> authentication services.
— <b>authorization</b> authorization services.
— <b>all</b> accounting, authentication, and authorization services.
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 248.
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 192; Arista User Manual, v. 4.11.1 (1/11/13), at 145; Arista User Manual v. 4.10.3 (10/22/12), at 137; Arista User Manual v. 4.9.3.2 (5/3/12), at 126; Arista User Manual v. 4.8.2 (11/18/11), at 115; Arista User Manual v. 4.7.3 (7/18/11), at 99.
</td>
</tr>
<tr>
<td>Cisco IOS 15.4
Effective date of registration: 11/26/2014</td>
<td>

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>snmp-server community</b></td><td>Specifies the community access string to define the relationship between the SNMP manager and the SNMP agent to permit access to SNMP.</td></tr>
<tr><td><b>snmp-server host</b></td><td>Specifies the recipient (host) of an SNMP notification operation.</td></tr>
</table>
Cisco IOS Security Command Reference: Commands S to Z at 1042 (2013).
</td>
<td>

<b>Configuring the Host</b>
The snmp-server host command specifies the recipient of a SNMP notification. An SNMP host is the recipient of an SNMP trap operation. The <b>snmp-server host</b> command sets the community string if it was not previously configured.
Arista User Manual v. 4.14.3F (Rev. 2)(10/2/2014), at 1967.
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1686; Arista User Manual, v. 4.11.1 (1/11/13), at 1344; Arista User Manual v. 4.10.3 (10/22/12), at 1110; Arista User Manual v. 4.9.3.2 (5/3/12), at 866; Arista User Manual v. 4.8.2 (11/18/11), at 677; Arista User Manual v. 4.7.3 (7/18/11), at 533.
</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	snmp-server enable traps ipsec
	To enable the router to send IP Security (IPSec) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps ipsec**command in global configuration mode. To disable IPSec SNMP notifications, use the **no**form of this command.
	snmp-server enable traps ipsec [**cryptomap** [**add**| **delete**| **attach**| **detach**]| **tunnel** [**start**| **stop**]| **too-many-sas**]
	no snmp-server enable traps ipsec [**cryptomap** [**add**| **delete**| **attach**| **detach**]| **tunnel** [**start**| **stop**]| **too-many-sas**]
	. . .
	
	SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.
	Cisco IOS Security Command Reference: Commands S to Z at 1044 - 1045 (2013).
		
		snmp-server enable traps
		The **snmp-server enable traps** command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The **snmp-server host** command specifies the notification type (traps or informs). Sending notifications requires at least one **snmp-server host** command.
		The **snmp-server enable traps** and **no snmp-server enable traps** commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The **default snmp-server enable traps** command resets notification generation to the default setting for the specified MIB.
		Platform all
		Command Mode Global Configuration
		Command Syntax
		`snmp-server enable traps[trap_type]`
		`no snmp-server enable traps [trap_type]`
		`default snmp-server enable traps [trap_type]`
		Arista User Manual v. 4.14.3F (Rev. 2) at 1990 (October 2, 2014).
		See also Arista User Manual v. 4.13.6F (4/14/2014), at 1918; Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.

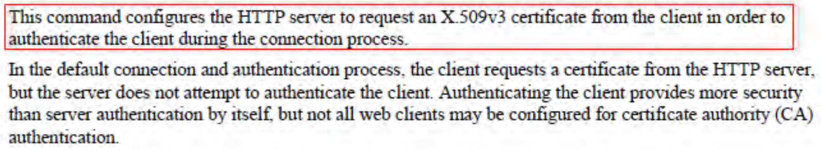
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>connect</b></td><td>Logs in to a host that supports Telnet, rlogin, or LAT.</td></tr>
<tr><td><b>kerberos clients mandatory</b></td><td>Causes the <b>rsh</b>, <b>rcp</b>, <b>rlogin</b>, and <b>telnet</b> commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.</td></tr>
<tr><td><b>name connection</b></td><td>Assigns a logical name to a connection.</td></tr>
<tr><td><b>rlogin</b></td><td>Logs in to a UNIX host using rlogin.</td></tr>
<tr><td><b>show hosts</b></td><td>Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.</td></tr>
<tr><td><b>show tcp</b></td><td>Displays the status of TCP connections.</td></tr>
</table>

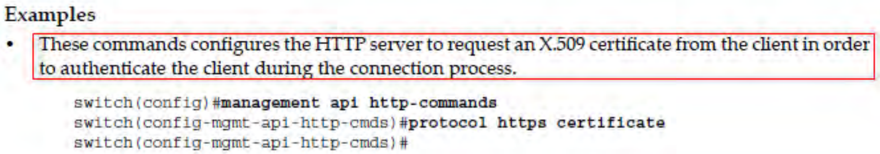
Cisco IOS Security Command Reference: Commands S to Z at 1192 (2013).
</td>
<td>

<b>show hosts</b>
The show hosts command displays the default domain name, name lookup service style, a list of name server hosts, and the static hostname-IP address maps.
Platform all
Command Mode EXEC
Command Syntax
<code>show hosts</code>

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 342.

<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 276; Arista User Manual, v. 4.11.1 (1/11/13), at 222; Arista User Manual v. 4.10.3 (10/22/12), at 191; Arista User Manual v. 4.9.3.2 (5/3/12), at 177.
</td>
</tr>
<tr>
<td>Cisco IOS 15.4

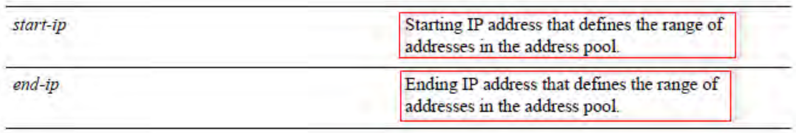
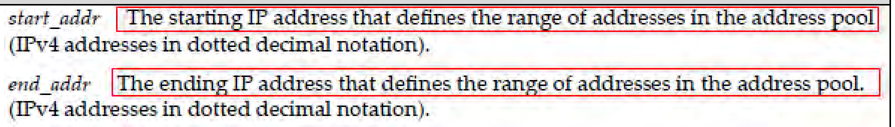
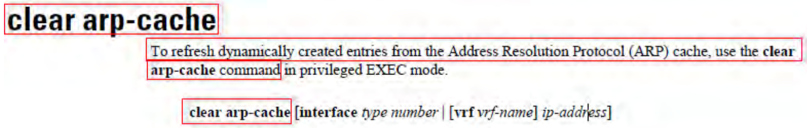
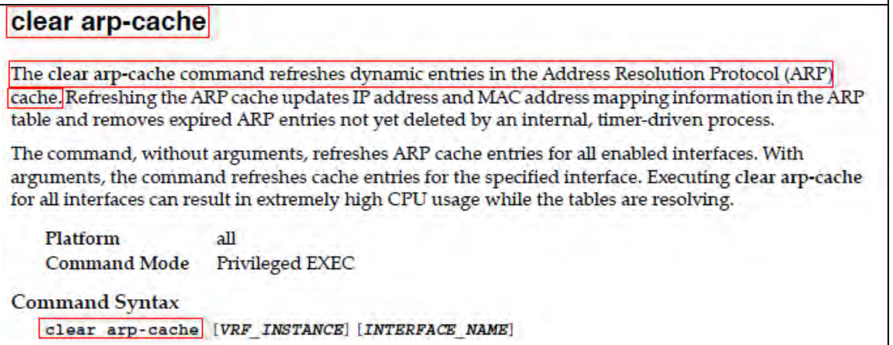
Effective date of registration: 11/26/2014</td>
<td>

This command configures the HTTP server to request an X.509v3 certificate from the client in order to authenticate the client during the connection process.

In the default connection and authentication process, the client requests a certificate from the HTTP server, but the server does not attempt to authenticate the client. Authenticating the client provides more security than server authentication by itself, but not all web clients may be configured for certificate authority (CA) authentication.

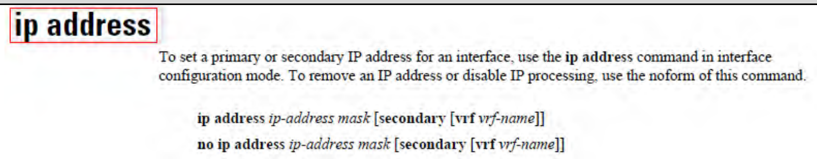
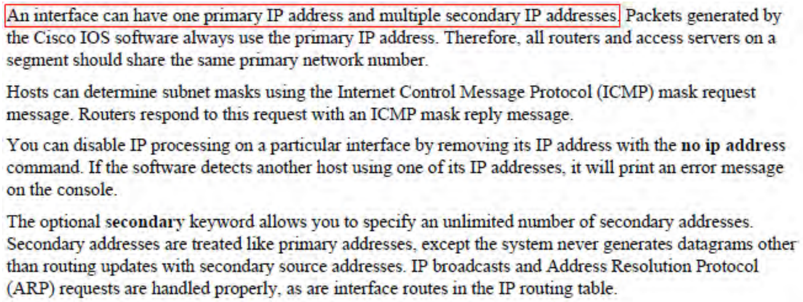
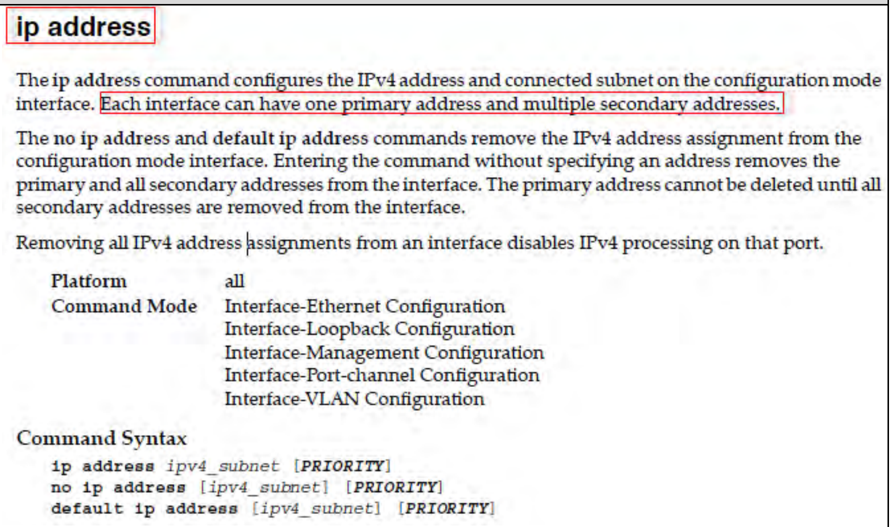
Cisco IOS HTTP Services Configuration Guide at 47 (2011).
</td>
<td>

Examples
• These commands configures the HTTP server to request an X.509 certificate from the client in order to authenticate the client during the connection process.
<code>switch(config)#<b>management api http-commands</b></code>
<code>switch(config-mgmt-api-http-cmds)#<b>protocol https certificate</b></code>
<code>switch(config-mgmt-api-http-cmds)#</code>

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 87.

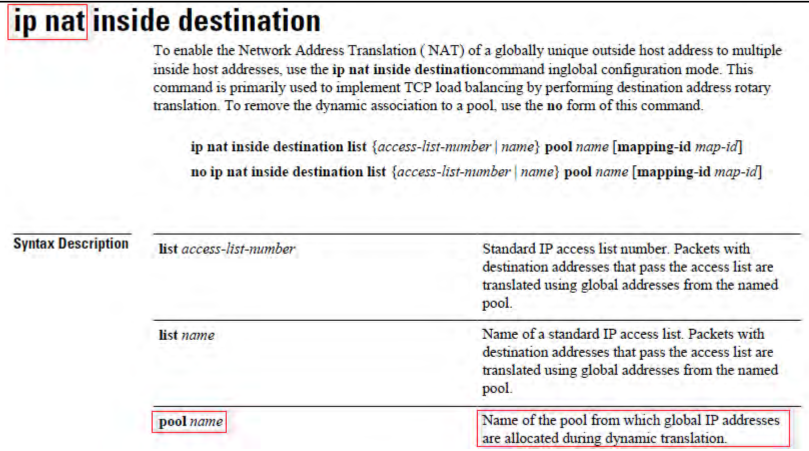
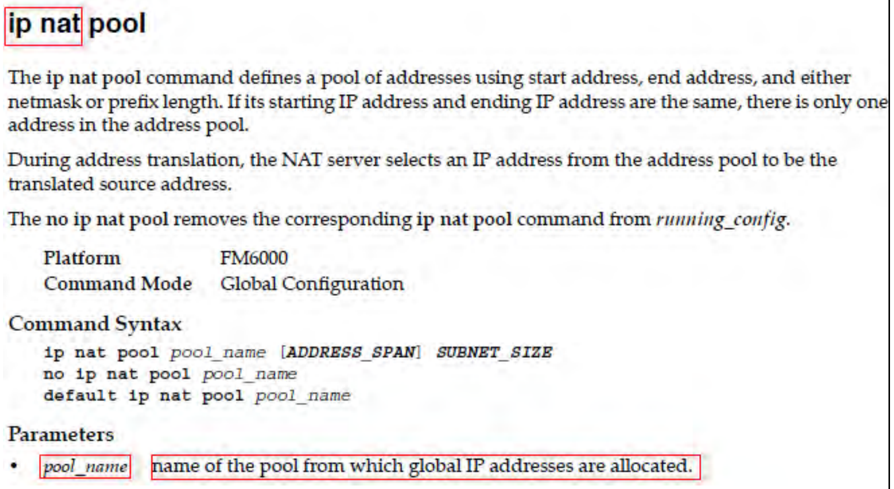
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 75.
</td>
</tr>
</table>

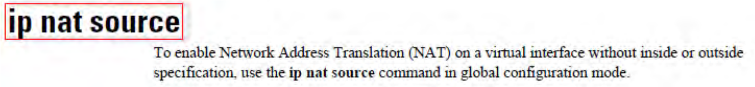
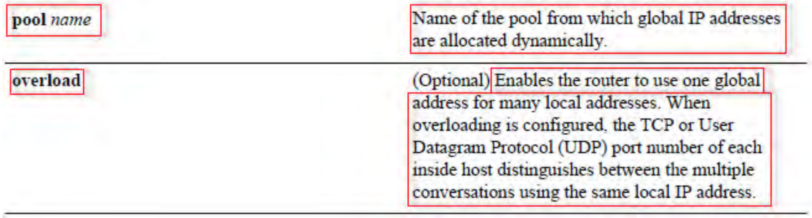
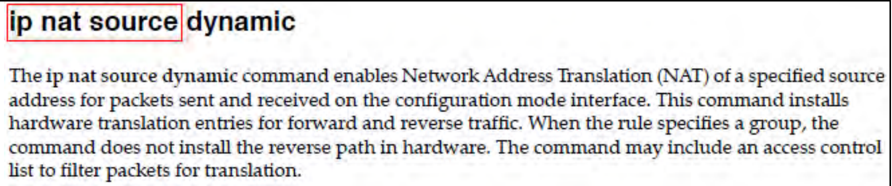
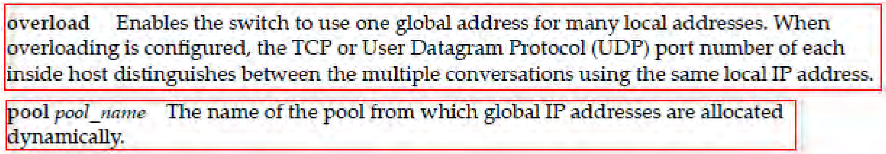
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 *start-ip* Starting IP address that defines the range of addresses in the address pool. *end-ip* Ending IP address that defines the range of addresses in the address pool. Cisco IOS IP Addressing Services Command Reference at 22 (2011).	 *start_addr* The starting IP address that defines the range of addresses in the address pool (IPv4 addresses in dotted decimal notation). *end_addr* The ending IP address that defines the range of addresses in the address pool. (IPv4 addresses in dotted decimal notation). Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1278. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1075.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **clear arp-cache** To refresh dynamically created entries from the Address Resolution Protocol (ARP) cache, use the **clear arp-cache** command in privileged EXEC mode. **clear arp-cache** [**interface** *type number* | [**vrf** *vrf-name*] *ip-address*] Cisco IOS IP Addressing Services Command Reference at 59 (2011).	 **clear arp-cache** The clear arp-cache command refreshes dynamic entries in the Address Resolution Protocol (ARP) cache. Refreshing the ARP cache updates IP address and MAC address mapping information in the ARP table and removes expired ARP entries not yet deleted by an internal, timer-driven process. The command, without arguments, refreshes ARP cache entries for all enabled interfaces. With arguments, the command refreshes cache entries for the specified interface. Executing clear arp-cache for all interfaces can result in extremely high CPU usage while the tables are resolving. Platform all Command Mode Privileged EXEC Command Syntax `clear arp-cache` [*VRF_INSTANCE*] [*INTERFACE_NAME*] Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1255. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1060; Arista User Manual, v. 4.11.1 (1/11/13), at 846; Arista User Manual v. 4.10.3 (10/22/12), at 692.

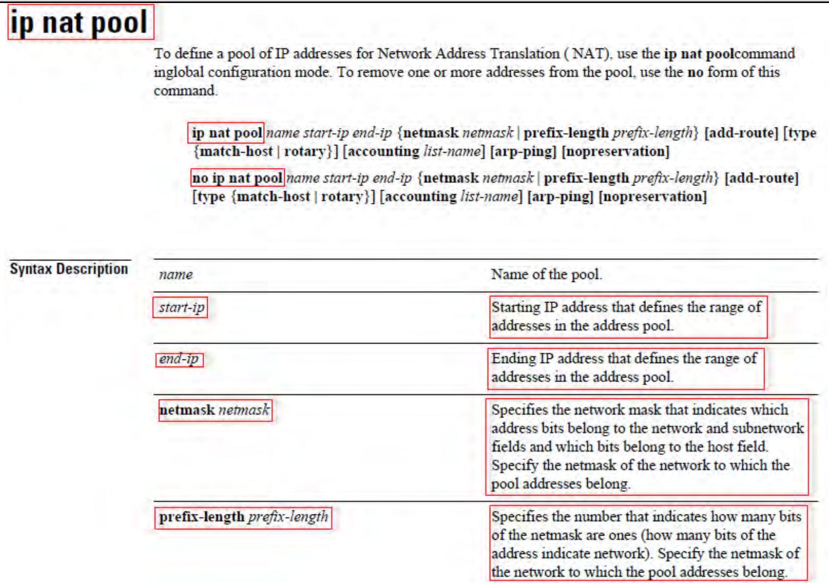
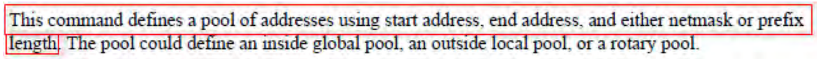
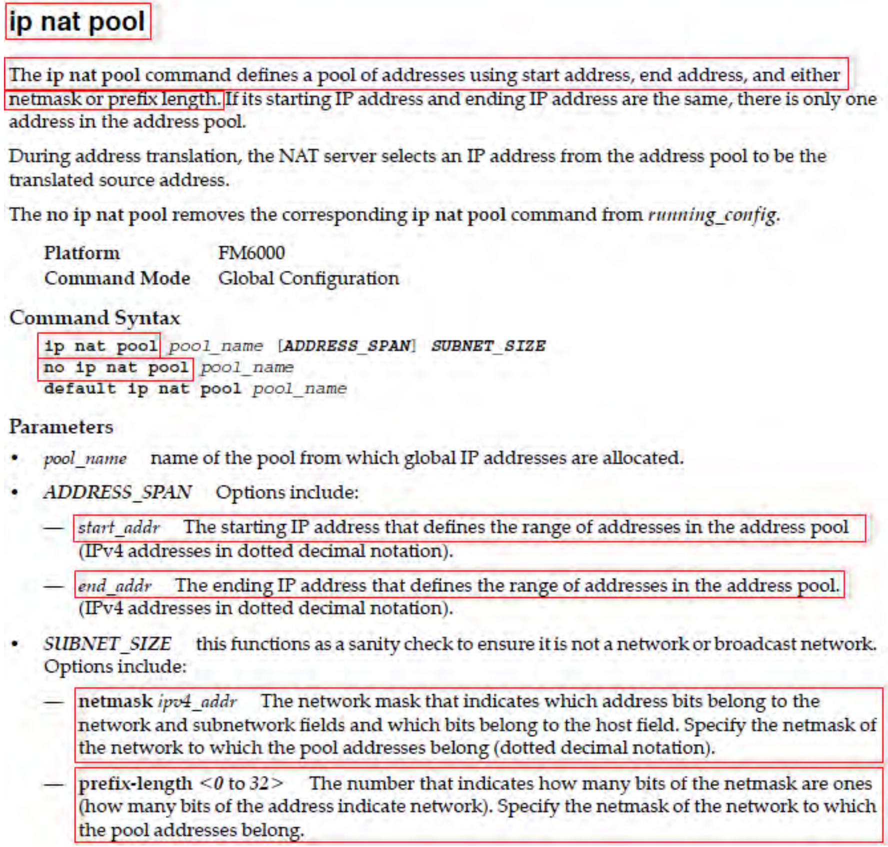
Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	ip address
	To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the noform of this command.
	ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
	no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
	Cisco IOS IP Addressing Services Command Reference at 166 (2011)
	
	An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.
	Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Routers respond to this request with an ICMP mask reply message.
	You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.
	The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.
	Cisco IOS IP Addressing Services Command Reference at 167 (2011).
		
		ip address
		The **ip address** command configures the IPv4 address and connected subnet on the configuration mode interface. Each interface can have one primary address and multiple secondary addresses.
		The **no ip address** and **default ip address** commands remove the IPv4 address assignment from the configuration mode interface. Entering the command without specifying an address removes the primary and all secondary addresses from the interface. The primary address cannot be deleted until all secondary addresses are removed from the interface.
		Removing all IPv4 address assignments from an interface disables IPv4 processing on that port.
		Platform all
		Command Mode Interface-Ethernet Configuration
		Interface-Loopback Configuration
		Interface-Management Configuration
		Interface-Port-channel Configuration
		Interface-VLAN Configuration
		Command Syntax
		`ip address ipv4_subnet [PRIORITY]`
		`no ip address [ipv4_subnet] [PRIORITY]`
		`default ip address [ipv4_subnet] [PRIORITY]`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1262.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1066; Arista User Manual, v. 4.11.1 (1/11/13), at 850; Arista User Manual v. 4.10.3 (10/22/12), at 696.

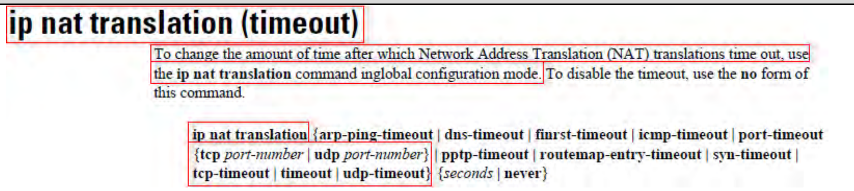
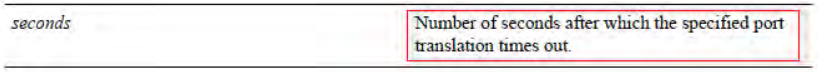
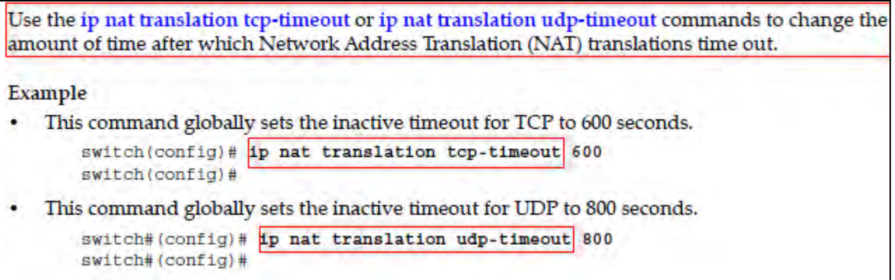
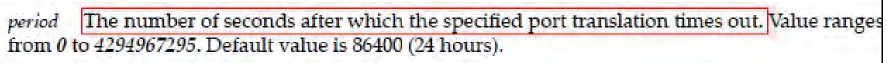
Copyright Registration Information	Cisco	Arista

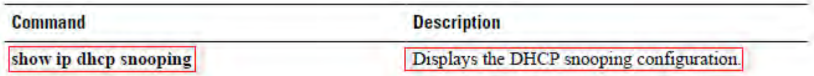
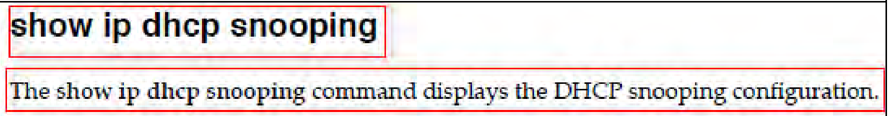
Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	ip nat inside destination
	To enable the Network Address Translation (NAT) of a globally unique outside host address to multiple inside host addresses, use the **ip nat inside destination**command inglobal configuration mode. This command is primarily used to implement TCP load balancing by performing destination address rotary translation. To remove the dynamic association to a pool, use the **no** form of this command.
	ip nat inside destination list {*access-list-number* | *name*} **pool** *name* [**mapping-id** *map-id*]
	no ip nat inside destination list {*access-list-number* | *name*} **pool** *name* [**mapping-id** *map-id*]
	Syntax Description
	list *access-list-number* — Standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
	list *name* — Name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
	pool *name* — Name of the pool from which global IP addresses are allocated during dynamic translation.
	Cisco IOS IP Addressing Services Command Reference at 405 (2011).
		
		ip nat pool
		The ip nat pool command defines a pool of addresses using start address, end address, and either netmask or prefix length. If its starting IP address and ending IP address are the same, there is only one address in the address pool.
		During address translation, the NAT server selects an IP address from the address pool to be the translated source address.
		The no ip nat pool removes the corresponding ip nat pool command from *running_config*.
		Platform FM6000
		Command Mode Global Configuration
		Command Syntax
		`ip nat pool pool_name [ADDRESS_SPAN] SUBNET_SIZE`
		`no ip nat pool pool_name`
		`default ip nat pool pool_name`
		Parameters
		• *pool_name* name of the pool from which global IP addresses are allocated.
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1278.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1075.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **ip nat source** To enable Network Address Translation (NAT) on a virtual interface without inside or outside specification, use the **ip nat source** command in global configuration mode. Cisco IOS IP Addressing Services Command Reference (2011), at 439.  **pool** *name* Name of the pool from which global IP addresses are allocated dynamically. **overload** (Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address. Cisco IOS IP Addressing Services Command Reference (2011), at 440.	 **ip nat source dynamic** The ip nat source dynamic command enables Network Address Translation (NAT) of a specified source address for packets sent and received on the configuration mode interface. This command installs hardware translation entries for forward and reverse traffic. When the rule specifies a group, the command does not install the reverse path in hardware. The command may include an access control list to filter packets for translation. . . .  overload Enables the switch to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address. pool *pool_name* The name of the pool from which global IP addresses are allocated dynamically. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/14), at 1279. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1076.

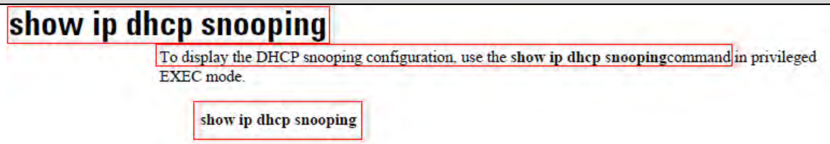
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **ip nat pool** To define a pool of IP addresses for Network Address Translation (NAT), use the **ip nat pool**command inglobal configuration mode. To remove one or more addresses from the pool, use the **no** form of this command. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} **[add-route] [type** {**match-host** | **rotary**}**] [accounting** *list-name*] **[arp-ping] [nopreservation]** **no ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} **[add-route] [type** {**match-host** | **rotary**}**] [accounting** *list-name*] **[arp-ping] [nopreservation]** **Syntax Description** *name* — Name of the pool. *start-ip* — Starting IP address that defines the range of addresses in the address pool. *end-ip* — Ending IP address that defines the range of addresses in the address pool. **netmask** *netmask* — Specifies the network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong. **prefix-length** *prefix-length* — Specifies the number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong. Cisco IOS IP Addressing Services Command Reference (2011), at 422.  This command defines a pool of addresses using start address, end address, and either netmask or prefix length. The pool could define an inside global pool, an outside local pool, or a rotary pool. Cisco IOS IP Addressing Services Command Reference (2011), at 423.	 **ip nat pool** The ip nat pool command defines a pool of addresses using start address, end address, and either netmask or prefix length. If its starting IP address and ending IP address are the same, there is only one address in the address pool. During address translation, the NAT server selects an IP address from the address pool to be the translated source address. The no ip nat pool removes the corresponding ip nat pool command from *running_config*. Platform FM6000 Command Mode Global Configuration **Command Syntax** `ip nat pool` *`pool_name`* **`[ADDRESS_SPAN]`** **`SUBNET_SIZE`** `no ip nat pool` *`pool_name`* `default ip nat pool` *`pool_name`* **Parameters** • *pool_name* name of the pool from which global IP addresses are allocated. • *ADDRESS_SPAN* Options include: — *start_addr* The starting IP address that defines the range of addresses in the address pool (IPv4 addresses in dotted decimal notation). — *end_addr* The ending IP address that defines the range of addresses in the address pool. (IPv4 addresses in dotted decimal notation). • *SUBNET_SIZE* this functions as a sanity check to ensure it is not a network or broadcast network. Options include: — **netmask** *ipv4_addr* The network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong (dotted decimal notation). — **prefix-length** *<0 to 32>* The number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1278. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1075.

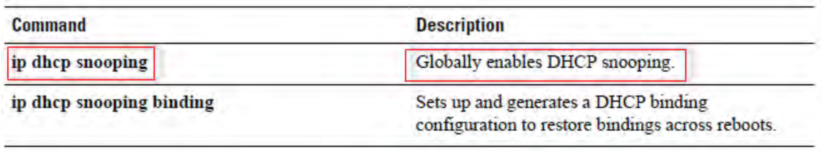
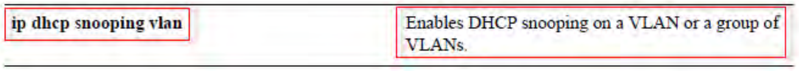
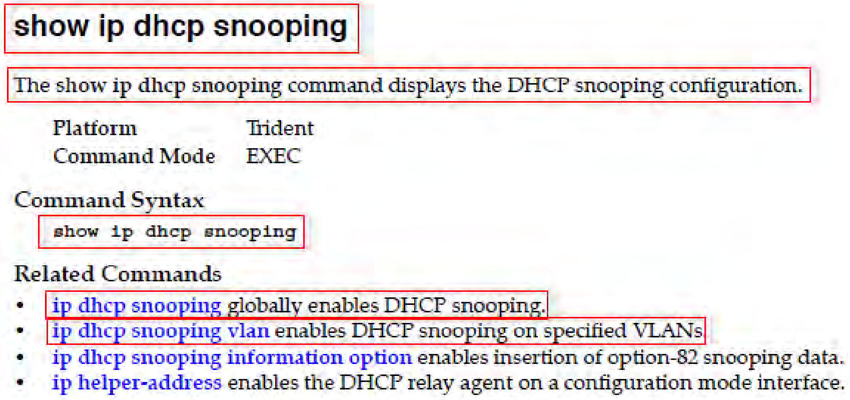
Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	ip nat translation (timeout)
	To change the amount of time after which Network Address Translation (NAT) translations time out, use the **ip nat translation** command inglobal configuration mode. To disable the timeout, use the **no** form of this command.
	ip nat translation {**arp-ping-timeout** | **dns-timeout** | **finrst-timeout** | **icmp-timeout** | **port-timeout** {**tcp** *port-number* | **udp** *port-number*} | **pptp-timeout** | **routemap-entry-timeout** | **syn-timeout** | **tcp-timeout** | **timeout** | **udp-timeout**} {*seconds* | **never**}
	Cisco IOS IP Addressing Services Command Reference (2011), at 446.
	
	seconds Number of seconds after which the specified port translation times out.
	Cisco IOS IP Addressing Services Command Reference (2011), at 447.
		
		Use the ip nat translation tcp-timeout or ip nat translation udp-timeout commands to change the amount of time after which Network Address Translation (NAT) translations time out.
		Example
		• This command globally sets the inactive timeout for TCP to 600 seconds.
		`switch(config)# ip nat translation tcp-timeout 600`
		`switch(config)#`
		• This command globally sets the inactive timeout for UDP to 800 seconds.
		`switch#(config)# ip nat translation udp-timeout 800`
		`switch#(config)#`
		Arista User Manual 4.14.3F (Rev. 2) (10/2/2014), at 1247
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1053.
		
		period The number of seconds after which the specified port translation times out. Value ranges from *0* to *4294967295*. Default value is 86400 (24 hours).
		Arista User Manual 4.14.3F (Rev. 2) (10/2/2014), at 1284
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1079.

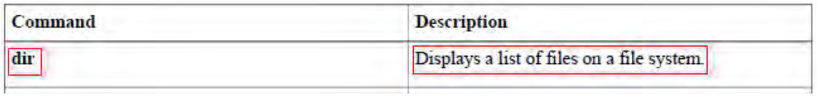
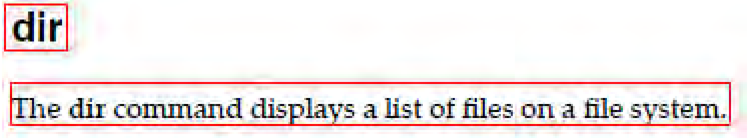
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Command** **Description** **show ip dhcp snooping** Displays the DHCP snooping configuration. Cisco IOS IP Addressing Services Command Reference (2011), at 311.	 **show ip dhcp snooping** The **show ip dhcp snooping** command displays the DHCP snooping configuration. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1302.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>
show ip dhcp snooping
To display the DHCP snooping configuration, use the show ip dhcp snoopingcommand in privileged EXEC mode.
show ip dhcp snooping

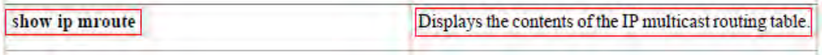
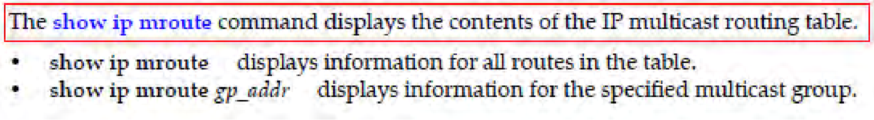
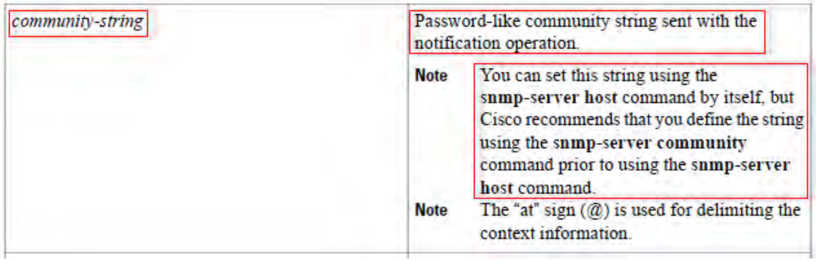
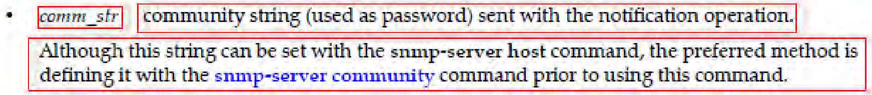
. . .

<table><tr><th>Command</th><th>Description</th></tr><tr><td>ip dhcp snooping</td><td>Globally enables DHCP snooping.</td></tr><tr><td>ip dhcp snooping binding</td><td>Sets up and generates a DHCP binding configuration to restore bindings across reboots.</td></tr></table>
Cisco IOS IP Addressing Services Command Reference (2011), at 673.

<table><tr><th></th><th></th></tr><tr><td>ip dhcp snooping vlan</td><td>Enables DHCP snooping on a VLAN or a group of VLANs.</td></tr></table>
Cisco IOS IP Addressing Services Command Reference (2011), at 674.</td>
<td>
show ip dhcp snooping
The show ip dhcp snooping command displays the DHCP snooping configuration.
Platform Trident
Command Mode EXEC
Command Syntax
show ip dhcp snooping
Related Commands
• ip dhcp snooping globally enables DHCP snooping.
• ip dhcp snooping vlan enables DHCP snooping on specified VLANs
• ip dhcp snooping information option enables insertion of option-82 snooping data.
• ip helper-address enables the DHCP relay agent on a configuration mode interface.

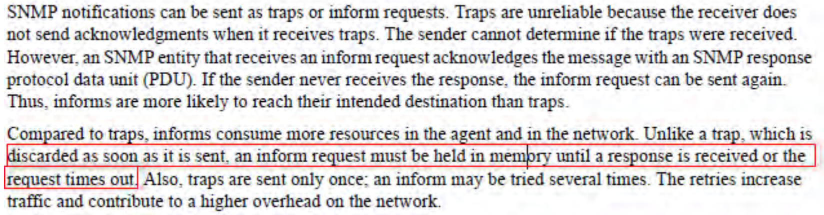
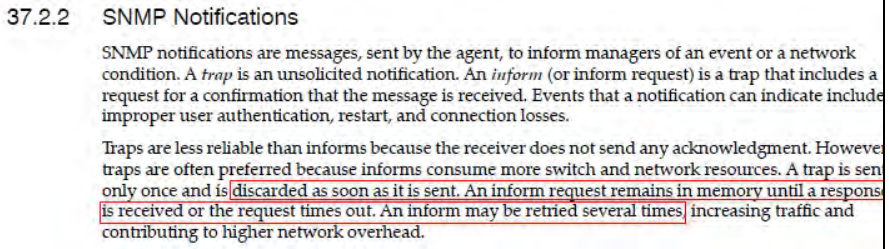
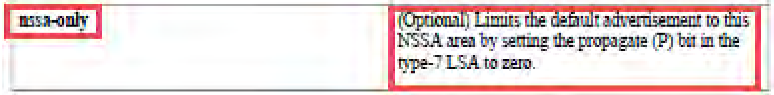
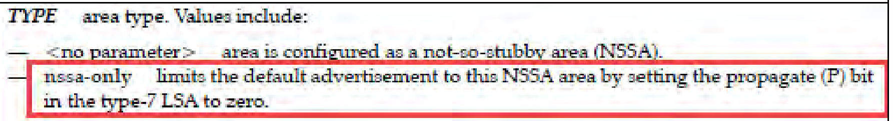
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1302.</td>
</tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>
<table><tr><th>Command</th><th>Description</th></tr><tr><td>dir</td><td>Displays a list of files on a file system.</td></tr></table>
Cisco IOS IP Application Services Command Reference (2013), at 283.</td>
<td>
dir
The dir command displays a list of files on a file system.

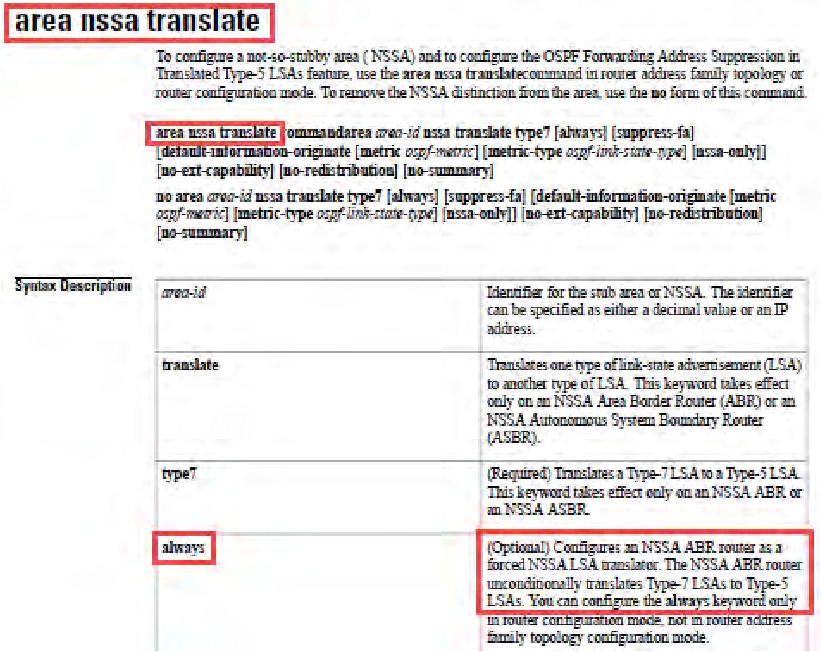
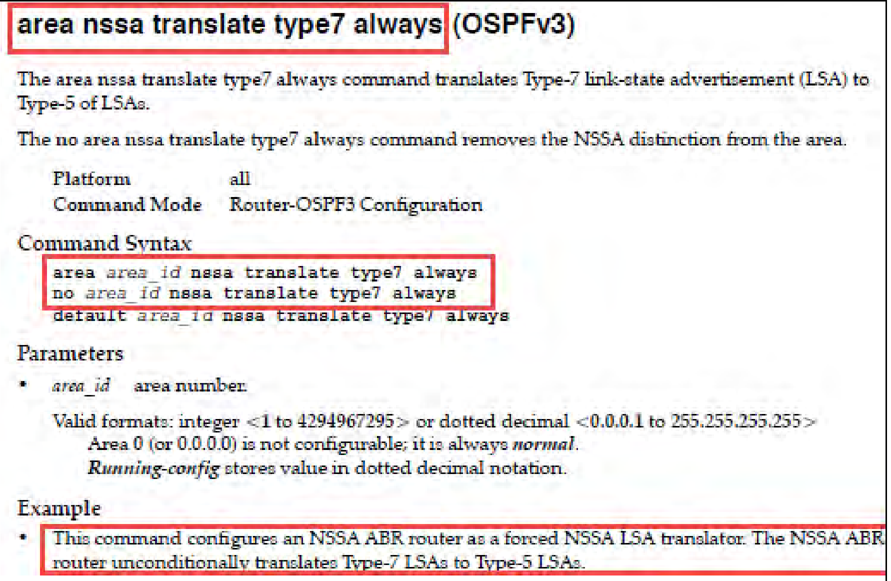
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 139

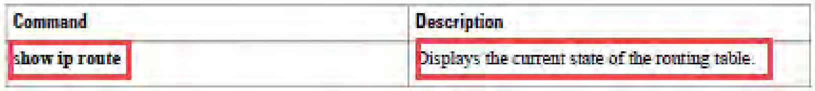
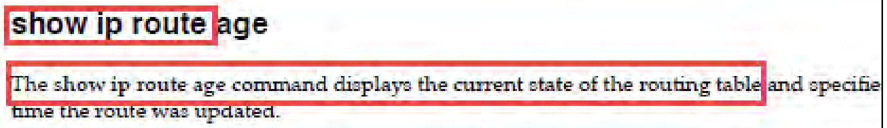
Arista User Manual v. 4.12.3 (7/17/13), at 115; Arista User Manual, v. 4.11.1 (1/11/13), at 55.</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 show ip mroute — Displays the contents of the IP multicast routing table. Cisco IOS IP Switching Command Reference (2013), at 483.	 The show ip mroute command displays the contents of the IP multicast routing table. • show ip mroute displays information for all routes in the table. • show ip mroute *gp_addr* displays information for the specified multicast group. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1757 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1485; Arista User Manual, v. 4.11.1 (1/11/13), at 1187; Arista User Manual v. 4.10.3 (10/22/12), at 1022; Arista User Manual v. 4.9.3.2 (5/3/12), at 780; Arista User Manual v. 4.8.2 (11/18/11), at 599.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 *community-string* — Password-like community string sent with the notification operation. Note You can set this string using the **snmp-server host** command by itself, but Cisco recommends that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command. Note The "at" sign (@) is used for delimiting the context information. Cisco IOS IP Switching Command Reference (2013), at 526.	 • *comm_str* community string (used as password) sent with the notification operation. Although this string can be set with the snmp-server host command, the preferred method is defining it with the snmp-server community command prior to using this command. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1995. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1685; Arista User Manual, v. 4.11.1 (1/11/13), at 1370; Arista User Manual v. 4.10.3 (10/22/12), at 1137; Arista User Manual v. 4.9.3.2 (5/3/12), at 893; Arista User Manual v. 4.8.2 (11/18/11), at 700; Arista User Manual v. 4.7.3 (7/18/11), at 479.

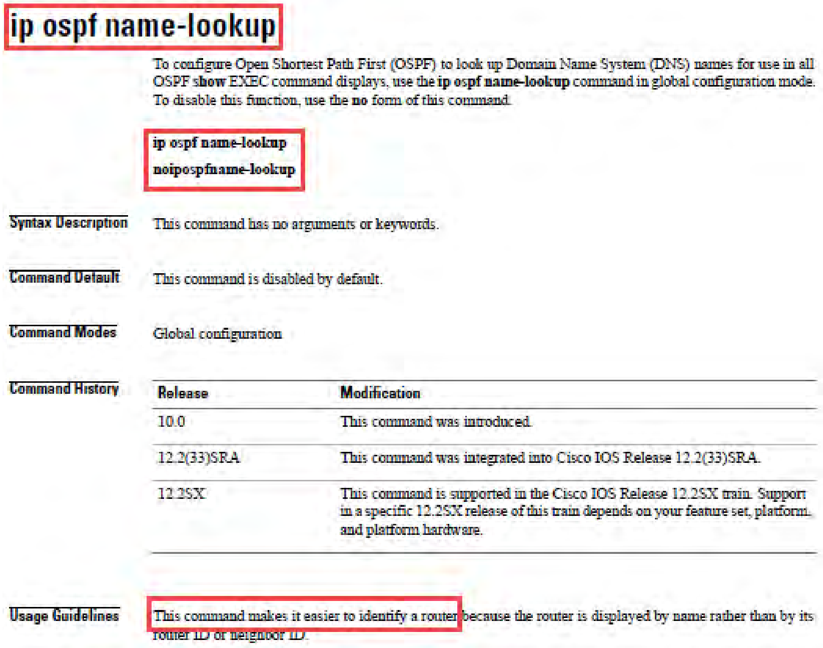
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination than traps. Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network. Cisco IOS IP Switching Command Reference (2013), at 530.	 37.2.2 SNMP Notifications SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A *trap* is an unsolicited notification. An *inform* (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses. Traps are less reliable than informs because the receiver does not send any acknowledgment. However traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1963, *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891;Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 nssa-only (Optional) Limits the default advertisement to this NSSA area by setting the propagate (P) bit in the type-7 LSA to zero. Cisco IOS IP Routing:OSPF Command Reference (2013), at 9.	 *TYPE* area type. Values include: — <no parameter> area is configured as a not-so-stubby area (NSSA). — nssa-only limits the default advertisement to this NSSA area by setting the propagate (P) bit in the type-7 LSA to zero. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/14), at 1498. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1283; Arista User Manual, v. 4.11.1 (1/11/13), at 958.

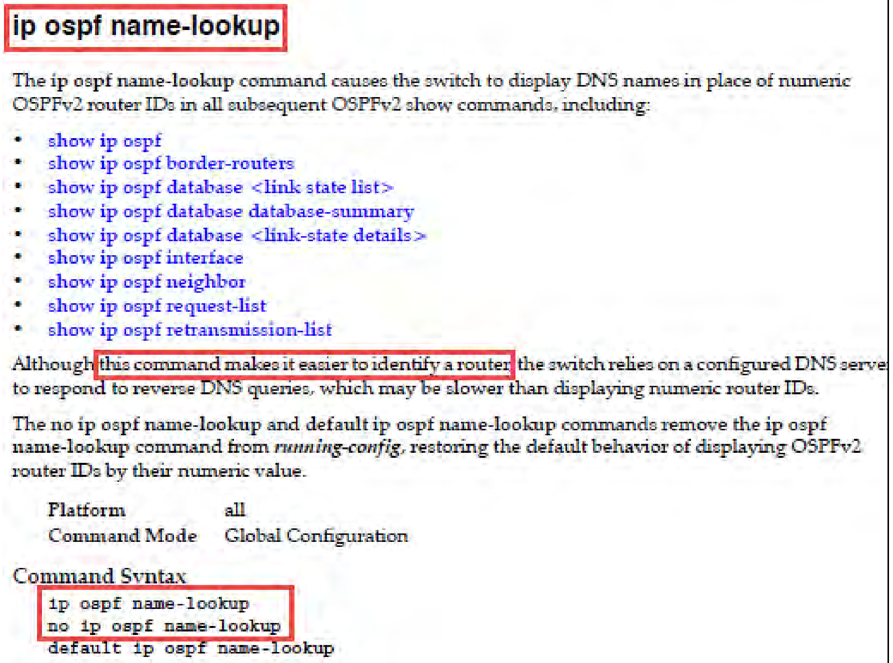
Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	area nssa translate
	To configure a not-so-stubby area (NSSA) and to configure the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature, use the **area nssa translate**command in router address family topology or router configuration mode. To remove the NSSA distinction from the area, use the **no** form of this command.
	area nssa translate **ommandarea** *area-id* **nssa translate type7** [**always**] [**suppress-fa**] [**default-information-originate** [**metric** *ospf-metric*] [**metric-type** *ospf-link-state-type*] [**nssa-only**]] [**no-ext-capability**] [**no-redistribution**] [**no-summary**]
	no area *area-id* **nssa translate type7** [**always**] [**suppress-fa**] [**default-information-originate** [**metric** *ospf-metric*] [**metric-type** *ospf-link-state-type*] [**nssa-only**]] [**no-ext-capability**] [**no-redistribution**] [**no-summary**]
	Syntax Description
	area-id — Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.
	translate — Translates one type of link-state advertisement (LSA) to another type of LSA. This keyword takes effect only on an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR).
	type7 — (Required) Translates a Type-7 LSA to a Type-5 LSA. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.
	always — (Optional) Configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. You can configure the **always** keyword only in router configuration mode, not in router address family topology configuration mode.
	Cisco IOS IP Routing:OSPF Command Reference (2013), at 11.
		
		area nssa translate type7 always (OSPFv3)
		The area nssa translate type7 always command translates Type-7 link-state advertisement (LSA) to Type-5 of LSAs.
		The no area nssa translate type7 always command removes the NSSA distinction from the area.
		Platform all
		Command Mode Router-OSPF3 Configuration
		Command Syntax
		`area area_id nssa translate type7 always`
		`no area_id nssa translate type7 always`
		`default area_id nssa translate type7 always`
		Parameters
		• *area_id* area number.
		Valid formats: integer <1 to 4294967295> or dotted decimal <0.0.0.1 to 255.255.255.255>
		Area 0 (or 0.0.0.0) is not configurable; it is always *normal*.
		Running-config stores value in dotted decimal notation.
		Example
		• This command configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs.
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1501.
		See also Arista User Manual v. 4.13.6F (4/14/2014), at 1451; Arista User Manual v. 4.12.3 (7/17/13), at 1286; Arista User Manual, v. 4.11.1 (1/11/13), at 1036.

Cisco IOS 15.4 Effective date of registration: 11/26/2014	 Command — Description **show ip route** — Displays the current state of the routing table. Cisco IOS IP Routing:OSPF Command Reference (2013), at 51.	 **show ip route age** The show ip route age command displays the current state of the routing table and specifie time the route was updated. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1313. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1102.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

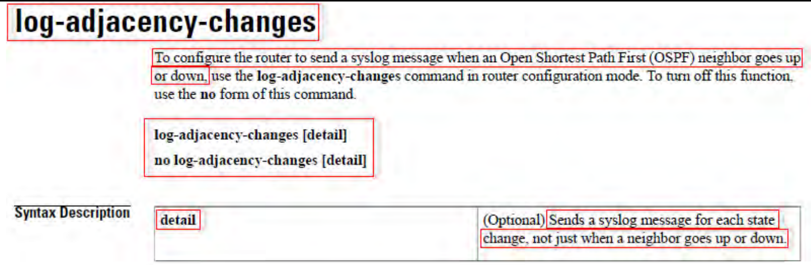
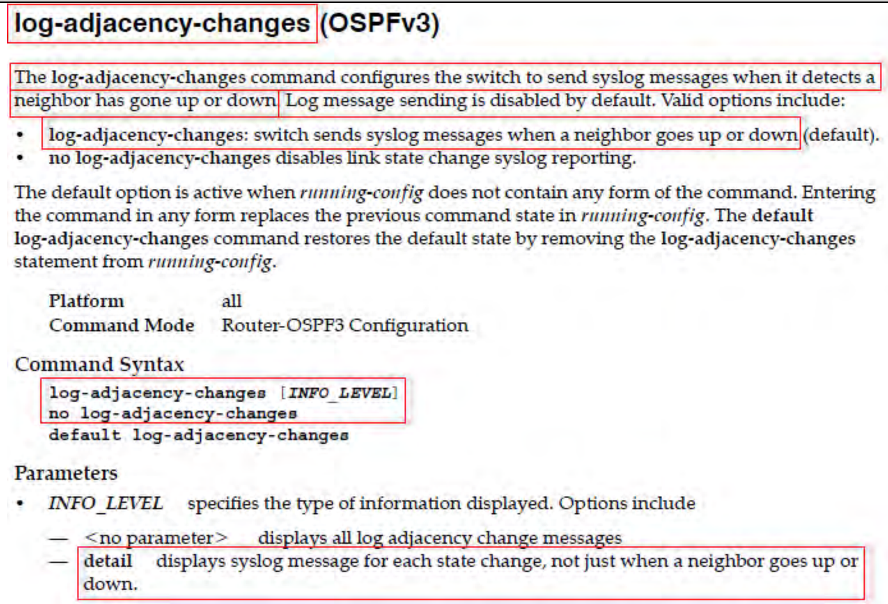
Effective date of registration: 11/26/2014</td>
<td>
ip ospf name-lookup
To configure Open Shortest Path First (OSPF) to look up Domain Name System (DNS) names for use in all OSPF **show** EXEC command displays, use the **ip ospf name-lookup** command in global configuration mode. To disable this function, use the **no** form of this command.
ip ospf name-lookup
noipospfname-lookup
Syntax Description: This command has no arguments or keywords.
Command Default: This command is disabled by default.
Command Modes: Global configuration
Command History: Release / Modification
10.0 — This command was introduced.
12.2(33)SRA — This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX — This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Usage Guidelines: This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

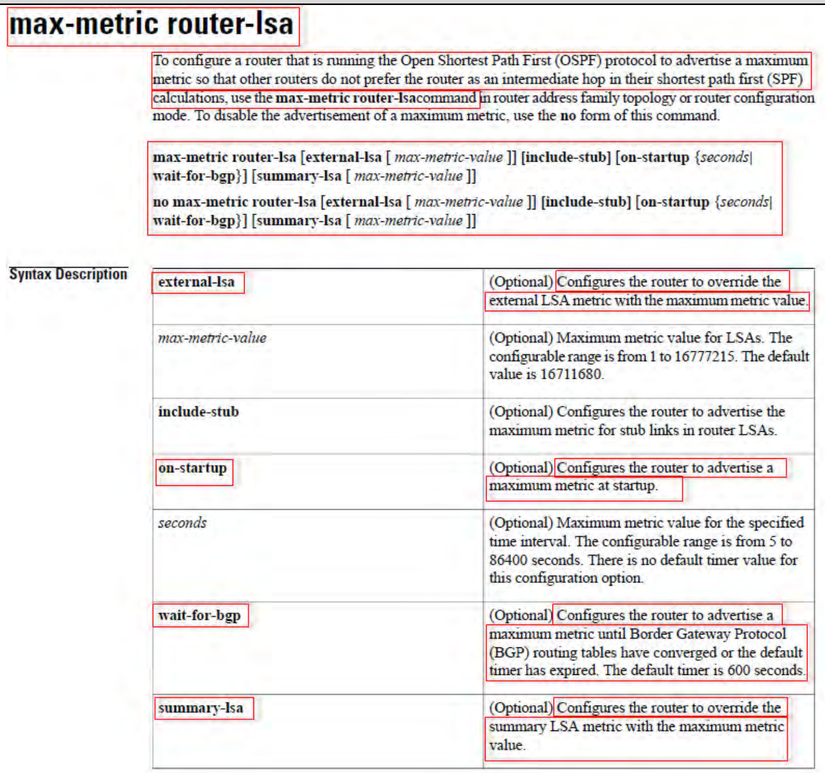
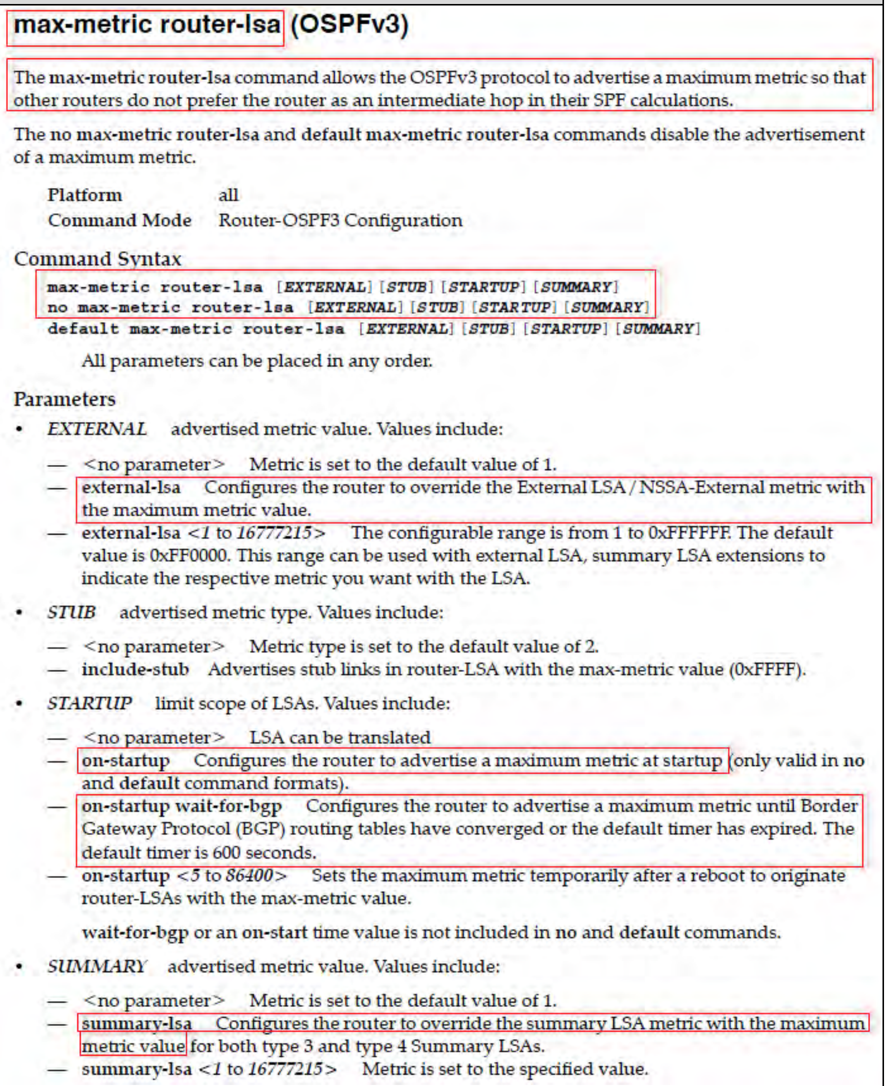
Cisco IOS IP Routing:OSPF Command Reference (2013), at 109.</td>
<td>
ip ospf name-lookup
The ip ospf name-lookup command causes the switch to display DNS names in place of numeric OSPFv2 router IDs in all subsequent OSPFv2 show commands, including:
• show ip ospf
• show ip ospf border-routers
• show ip ospf database &lt;link state list&gt;
• show ip ospf database database-summary
• show ip ospf database &lt;link-state details&gt;
• show ip ospf interface
• show ip ospf neighbor
• show ip ospf request-list
• show ip ospf retransmission-list
Although this command makes it easier to identify a router the switch relies on a configured DNS serve to respond to reverse DNS queries, which may be slower than displaying numeric router IDs.
The no ip ospf name-lookup and default ip ospf name-lookup commands remove the ip ospf name-lookup command from *running-config*, restoring the default behavior of displaying OSPFv2 router IDs by their numeric value.
Platform: all
Command Mode: Global Configuration
Command Syntax
`ip ospf name-lookup`
`no ip ospf name-lookup`
`default ip ospf name-lookup`

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1431.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1218; Arista User Manual, v. 4.11.1 (1/11/13), at 975; Arista User Manual v. 4.10.3 (10/22/12), at 805; Arista User Manual v. 4.9.3.2 (5/3/12), at 628; Arista User Manual v. 4.8.2 (11/18/11), at 464; Arista User Manual v. 4.7.3 (7/18/11), at 337; Arista User Manual v. 4.6.0 (12/22/2010), at 200.</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	log-adjacency-changes
	To configure the router to send a syslog message when an Open Shortest Path First (OSPF) neighbor goes up or down, use the **log-adjacency-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.
	log-adjacency-changes [detail]
	no log-adjacency-changes [detail]
	Syntax Description — **detail** — (Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.
	Cisco IOS IP Routing:OSPF Command Reference (2013), at 131.
		
		log-adjacency-changes (OSPFv3)
		The log-adjacency-changes command configures the switch to send syslog messages when it detects a neighbor has gone up or down. Log message sending is disabled by default. Valid options include:
		• log-adjacency-changes: switch sends syslog messages when a neighbor goes up or down (default).
		• no log-adjacency-changes disables link state change syslog reporting.
		The default option is active when *running-config* does not contain any form of the command. Entering the command in any form replaces the previous command state in *running-config*. The default log-adjacency-changes command restores the default state by removing the log-adjacency-changes statement from *running-config*.
		Platform all
		Command Mode Router-OSPF3 Configuration
		Command Syntax
		`log-adjacency-changes [INFO_LEVEL]`
		`no log-adjacency-changes`
		`default log-adjacency-changes`
		Parameters
		• *INFO_LEVEL* specifies the type of information displayed. Options include
		— <no parameter> displays all log adjacency change messages
		— detail displays syslog message for each state change, not just when a neighbor goes up or down.
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1518.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1303; Arista User Manual, v. 4.11.1 (1/11/13), at 1054; Arista User Manual v. 4.10.3 (10/22/12), at 811.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 Cisco IOS IP Routing:OSPF Command Reference (2013), at 136.	 Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1519.

max-metric router-lsa

To configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the **max-metric router-lsa**command in router address family topology or router configuration mode. To disable the advertisement of a maximum metric, use the **no** form of this command.

max-metric router-lsa [external-lsa [*max-metric-value*]] **[include-stub] [on-startup** {*seconds*| **wait-for-bgp**}] **[summary-lsa** [*max-metric-value*]]

no max-metric router-lsa [external-lsa [*max-metric-value*]] **[include-stub] [on-startup** {*seconds*| **wait-for-bgp**}] **[summary-lsa** [*max-metric-value*]]

Syntax Description

external-lsa	(Optional) Configures the router to override the external LSA metric with the maximum metric value.
max-metric-value	(Optional) Maximum metric value for LSAs. The configurable range is from 1 to 16777215. The default value is 16711680.
include-stub	(Optional) Configures the router to advertise the maximum metric for stub links in router LSAs.
on-startup	(Optional) Configures the router to advertise a maximum metric at startup.
seconds	(Optional) Maximum metric value for the specified time interval. The configurable range is from 5 to 86400 seconds. There is no default timer value for this configuration option.
wait-for-bgp	(Optional) Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.
summary-lsa	(Optional) Configures the router to override the summary LSA metric with the maximum metric value.

max-metric router-lsa (OSPFv3)

The **max-metric router-lsa** command allows the OSPFv3 protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.

The **no max-metric router-lsa** and **default max-metric router-lsa** commands disable the advertisement of a maximum metric.

Platform	all
Command Mode	Router-OSPF3 Configuration

Command Syntax

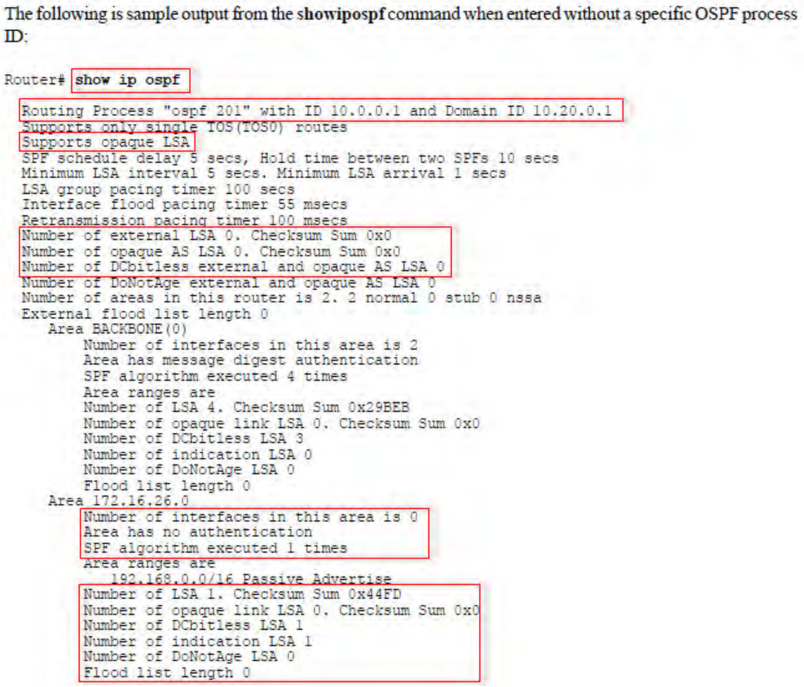
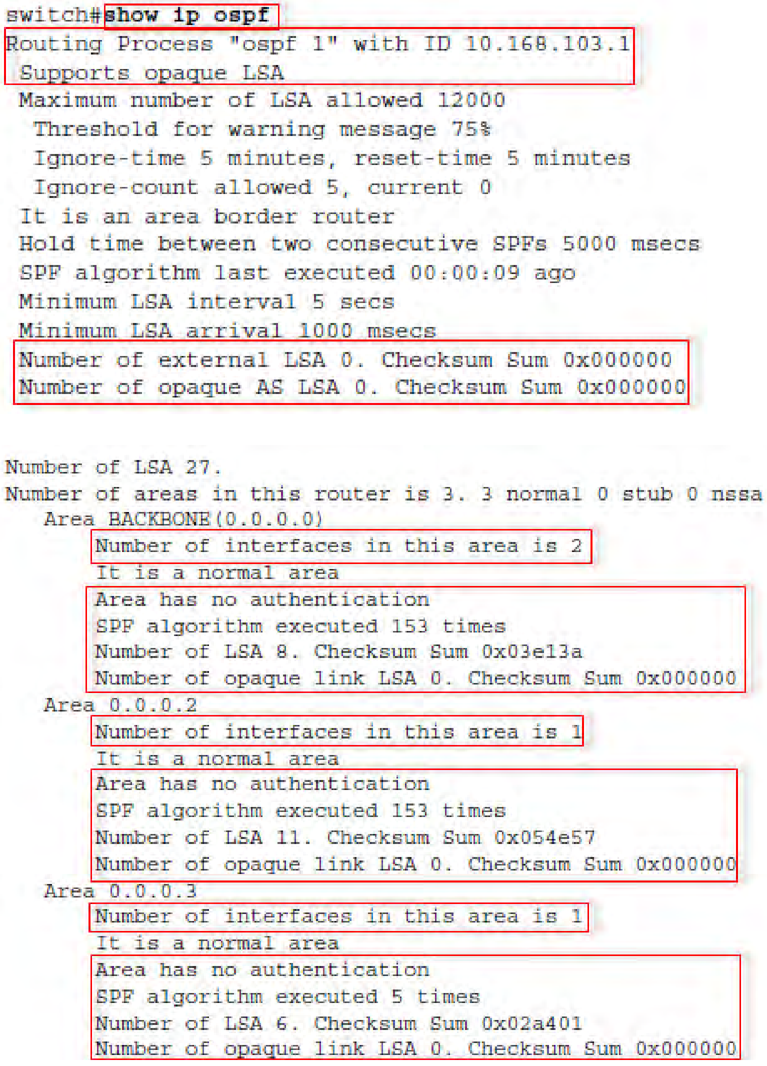
```
max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]
no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]
default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]
```

All parameters can be placed in any order.

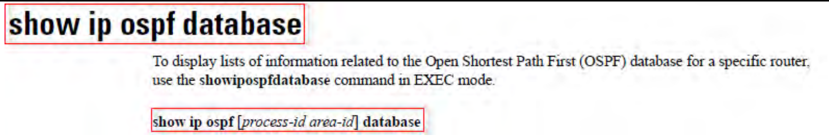
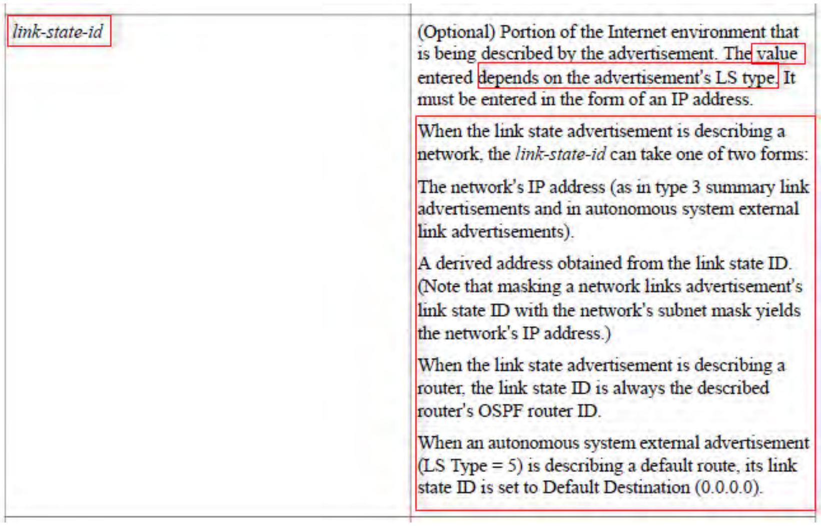
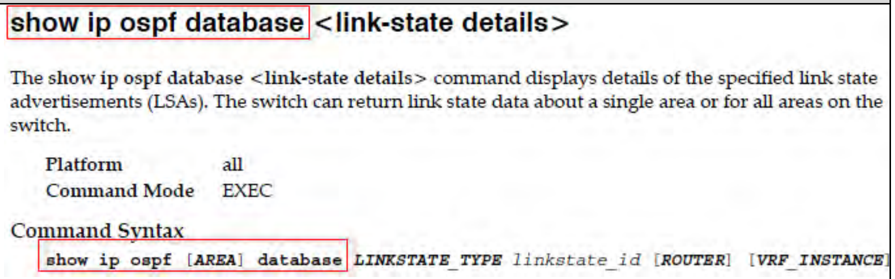
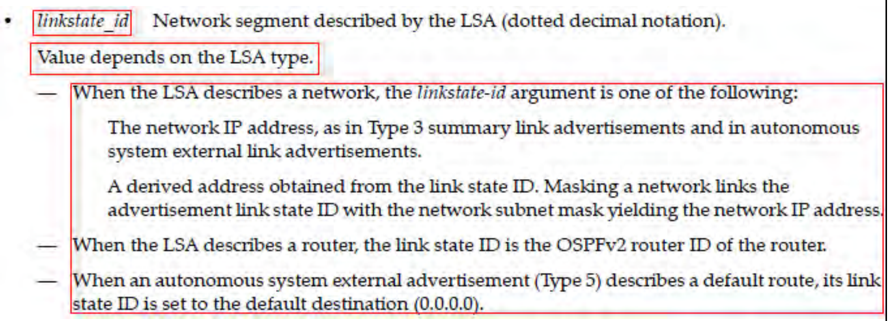
Parameters

- *EXTERNAL* advertised metric value. Values include:
  - — <no parameter> Metric is set to the default value of 1.
  - — **external-lsa** Configures the router to override the External LSA / NSSA-External metric with the maximum metric value.
  - — **external-lsa** <*1* to *16777215*> The configurable range is from 1 to 0xFFFFFF. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA.
- *STUB* advertised metric type. Values include:
  - — <no parameter> Metric type is set to the default value of 2.
  - — **include-stub** Advertises stub links in router-LSA with the max-metric value (0xFFFF).
- *STARTUP* limit scope of LSAs. Values include:
  - — <no parameter> LSA can be translated
  - — **on-startup** Configures the router to advertise a maximum metric at startup (only valid in **no** and **default** command formats).
  - — **on-startup wait-for-bgp** Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.
  - — **on-startup** <*5* to *86400*> Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value.

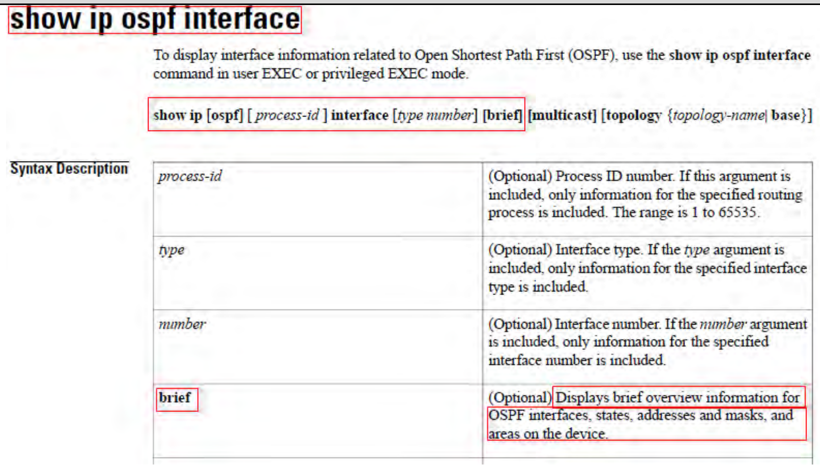
    wait-for-bgp or an **on-start** time value is not included in **no** and **default** commands.
- *SUMMARY* advertised metric value. Values include:
  - — <no parameter> Metric is set to the default value of 1.
  - — **summary-lsa** Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs.
  - — **summary-lsa** <*1* to *16777215*> Metric is set to the specified value.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 The following is sample output from the **showipospf** command when entered without a specific OSPF process ID: Router# **show ip ospf** Routing Process "ospf 201" with ID 10.0.0.1 and Domain ID 10.20.0.1 Supports only single TOS(TOS0) routes Supports opaque LSA SPF schedule delay 5 secs, Hold time between two SPFs 10 secs Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs LSA group pacing timer 100 secs Interface flood pacing timer 55 msecs Retransmission pacing timer 100 msecs Number of external LSA 0. Checksum Sum 0x0 Number of opaque AS LSA 0. Checksum Sum 0x0 Number of DCbitless external and opaque AS LSA 0 Number of DoNotAge external and opaque AS LSA 0 Number of areas in this router is 2. 2 normal 0 stub 0 nssa External flood list length 0 Area BACKBONE(0) Number of interfaces in this area is 2 Area has message digest authentication SPF algorithm executed 4 times Area ranges are Number of LSA 4. Checksum Sum 0x29BEB Number of opaque link LSA 0. Checksum Sum 0x0 Number of DCbitless LSA 3 Number of indication LSA 0 Number of DoNotAge LSA 0 Flood list length 0 Area 172.16.26.0 Number of interfaces in this area is 0 Area has no authentication SPF algorithm executed 1 times Area ranges are 192.168.0.0/16 Passive Advertise Number of LSA 1. Checksum Sum 0x44FD Number of opaque link LSA 0. Checksum Sum 0x0 Number of DCbitless LSA 1 Number of indication LSA 1 Number of DoNotAge LSA 0 Flood list length 0 Cisco IOS IP Routing:OSPF Command Reference (2013), at 174.	 switch#**show ip ospf** Routing Process "ospf 1" with ID 10.168.103.1 Supports opaque LSA Maximum number of LSA allowed 12000 Threshold for warning message 75% Ignore-time 5 minutes, reset-time 5 minutes Ignore-count allowed 5, current 0 It is an area border router Hold time between two consecutive SPFs 5000 msecs SPF algorithm last executed 00:00:09 ago Minimum LSA interval 5 secs Minimum LSA arrival 1000 msecs Number of external LSA 0. Checksum Sum 0x000000 Number of opaque AS LSA 0. Checksum Sum 0x000000 Number of LSA 27. Number of areas in this router is 3. 3 normal 0 stub 0 nssa Area BACKBONE(0.0.0.0) Number of interfaces in this area is 2 It is a normal area Area has no authentication SPF algorithm executed 153 times Number of LSA 8. Checksum Sum 0x03e13a Number of opaque link LSA 0. Checksum Sum 0x000000 Area 0.0.0.2 Number of interfaces in this area is 1 It is a normal area Area has no authentication SPF algorithm executed 153 times Number of LSA 11. Checksum Sum 0x054e57 Number of opaque link LSA 0. Checksum Sum 0x000000 Area 0.0.0.3 Number of interfaces in this area is 1 It is a normal area Area has no authentication SPF algorithm executed 5 times Number of LSA 6. Checksum Sum 0x02a401 Number of opaque link LSA 0. Checksum Sum 0x000000 Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1391-1392.

Copyright Registration Information	Cisco	Arista
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1180; Arista User Manual, v. 4.11.1 (1/11/13), at 939; Arista User Manual v. 4.10.3 (10/22/12), at 775; Arista User Manual v. 4.9.3.2 (5/3/12), at 645; Arista User Manual v. 4.8.2 (11/18/11), at 480; Arista User Manual v. 4.7.3 (7/18/11), at 353; Arista User Manual v. 4.6.0 (12/22/2010), at 213.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **show ip ospf database** To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the showipospfdatabase command in EXEC mode. **show ip ospf** [*process-id area-id*] **database** Cisco IOS IP Routing:OSPF Command Reference (2013), at 184  *link-state-id* (Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address. When the link state advertisement is describing a network, the *link-state-id* can take one of two forms: The network's IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements). A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.) When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID. When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0). Cisco IOS IP Routing:OSPF Command Reference (2013), at 185.	 **show ip ospf database** **<link-state details>** The **show ip ospf database <link-state details>** command displays details of the specified link state advertisements (LSAs). The switch can return link state data about a single area or for all areas on the switch. Platform all Command Mode EXEC Command Syntax `show ip ospf [AREA] database LINKSTATE_TYPE linkstate_id [ROUTER] [VRF_INSTANCE]` . . .  • *linkstate_id* Network segment described by the LSA (dotted decimal notation). Value depends on the LSA type. — When the LSA describes a network, the *linkstate-id* argument is one of the following: The network IP address, as in Type 3 summary link advertisements and in autonomous system external link advertisements. A derived address obtained from the link state ID. Masking a network links the advertisement link state ID with the network subnet mask yielding the network IP address. — When the LSA describes a router, the link state ID is the OSPFv2 router ID of the router. — When an autonomous system external advertisement (Type 5) describes a default route, its link state ID is set to the default destination (0.0.0.0). Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1454. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1404; Arista User Manual v. 4.12.3 (7/17/13), at 1240; Arista User Manual, v. 4.11.1 (1/11/13), at 996; Arista User Manual v. 4.10.3 (10/22/12), at 825; Arista User Manual v. 4.9.3.2 (5/3/12), at 647; Arista User Manual v. 4.8.2 (11/18/11), at 483; Arista User Manual v. 4.7.3 (7/18/11), at 357; Arista User Manual v. 4.6.0 (12/22/2010), at 217.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

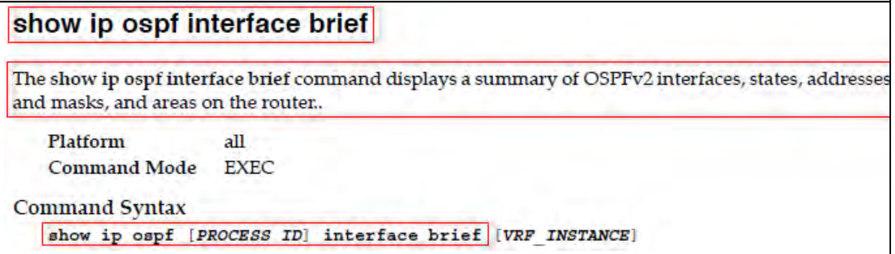
Effective date of registration: 11/26/2014</td>
<td>


<b>show ip ospf interface</b>

To display interface information related to Open Shortest Path First (OSPF), use the <b>show ip ospf interface</b> command in user EXEC or privileged EXEC mode.

<b>show ip [ospf] [</b> <i>process-id</i> <b>] interface [</b><i>type number</i><b>] [brief] [multicast] [topology</b> {<i>topology-name</i>| <b>base</b>}<b>]</b>

<b>Syntax Description</b>
<table>
<tr><td><i>process-id</i></td><td>(Optional) Process ID number. If this argument is included, only information for the specified routing process is included. The range is 1 to 65535.</td></tr>
<tr><td><i>type</i></td><td>(Optional) Interface type. If the <i>type</i> argument is included, only information for the specified interface type is included.</td></tr>
<tr><td><i>number</i></td><td>(Optional) Interface number. If the <i>number</i> argument is included, only information for the specified interface number is included.</td></tr>
<tr><td><b>brief</b></td><td>(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the device.</td></tr>
</table>

Cisco IOS IP Routing:OSPF Command Reference (2013), at 202.
</td>
<td>


<b>show ip ospf interface brief</b>

The show ip ospf interface brief command displays a summary of OSPFv2 interfaces, states, addresses and masks, and areas on the router..

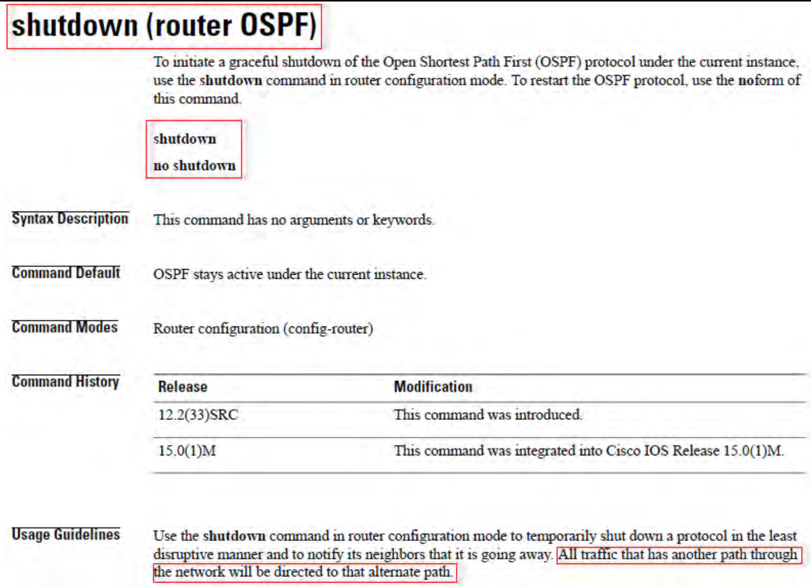
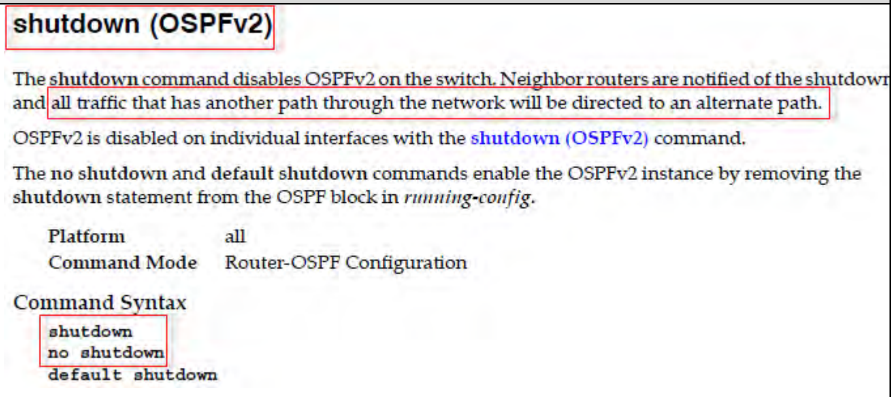
Platform all
Command Mode EXEC

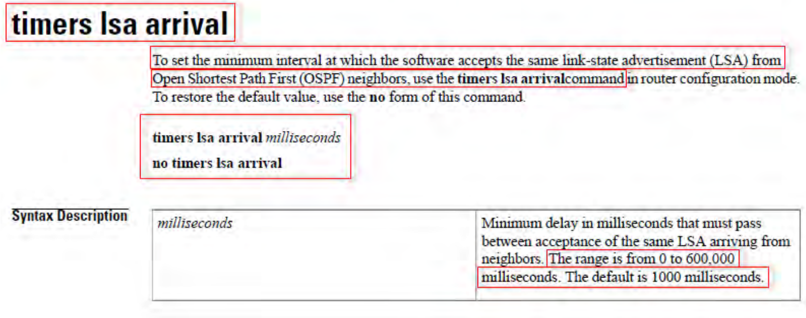
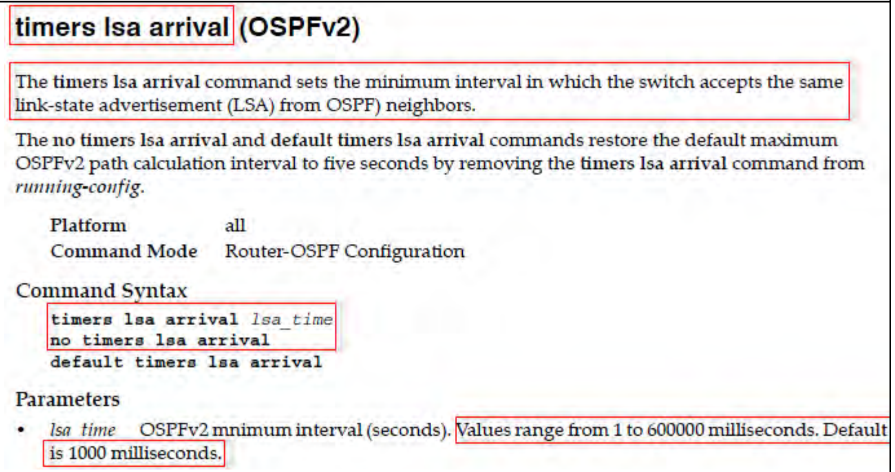
Command Syntax
<code>show ip ospf [PROCESS ID] interface brief [VRF_INSTANCE]</code>

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1458.

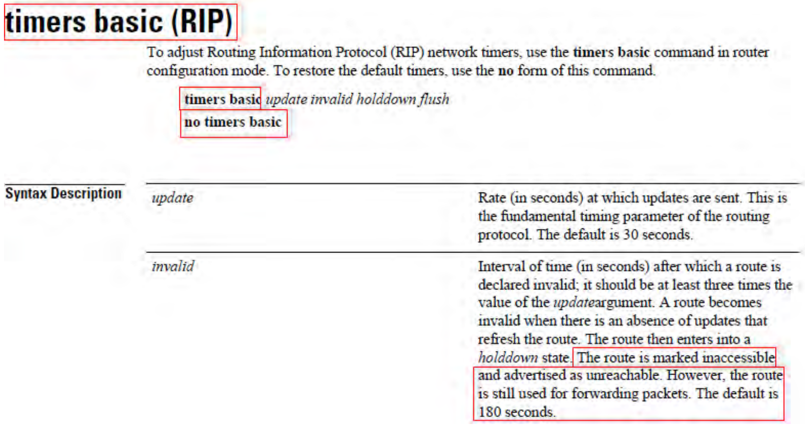
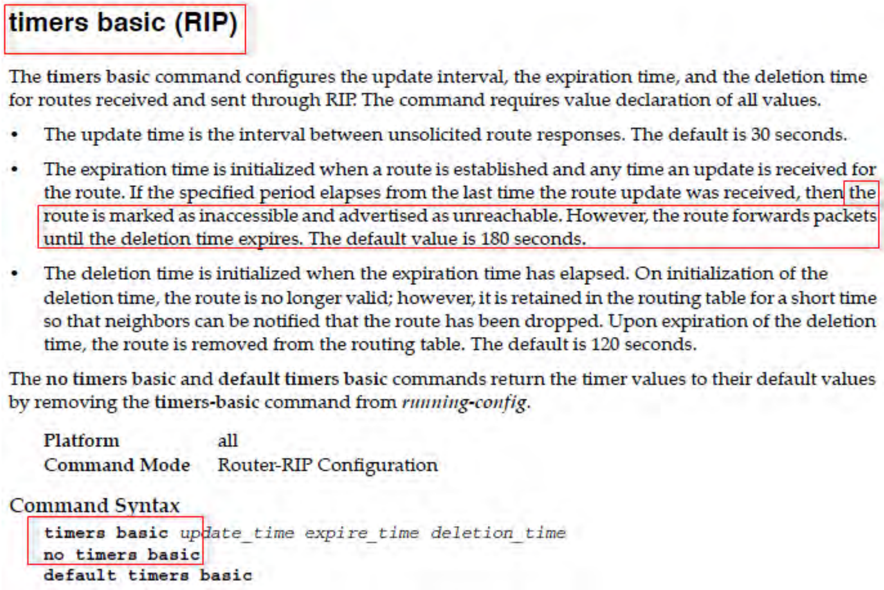
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1244; Arista User Manual, v. 4.11.1 (1/11/13), at 1000; Arista User Manual v. 4.10.3 (10/22/12), at 829; Arista User Manual v. 4.9.3.2 (5/3/12), at 653; Arista User Manual v. 4.8.2 (11/18/11), at 488; Arista User Manual v. 4.7.3 (7/18/11), at 360.
</td>
</tr>
</table>

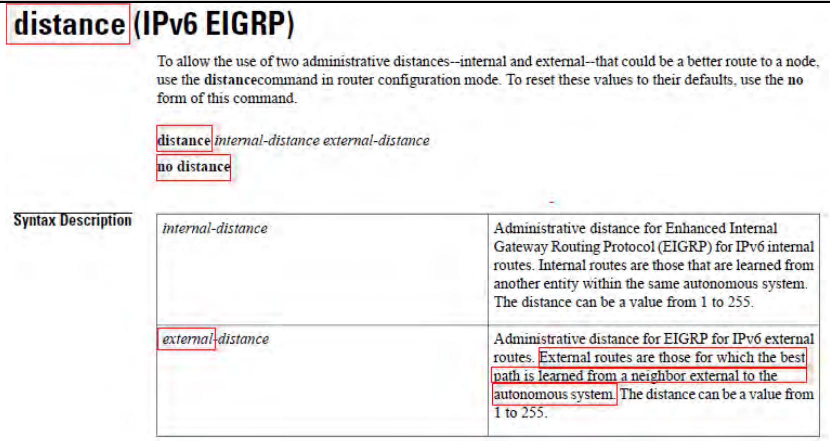
Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	shutdown (router OSPF)
	To initiate a graceful shutdown of the Open Shortest Path First (OSPF) protocol under the current instance, use the **shutdown** command in router configuration mode. To restart the OSPF protocol, use the **no**form of this command.
	`shutdown`
	`no shutdown`
	Syntax Description This command has no arguments or keywords.
	Command Default OSPF stays active under the current instance.
	Command Modes Router configuration (config-router)
	Command History **Release** / **Modification**
	12.2(33)SRC / This command was introduced.
	15.0(1)M / This command was integrated into Cisco IOS Release 15.0(1)M.
	Usage Guidelines Use the **shutdown** command in router configuration mode to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path.
	Cisco IOS IP Routing:OSPF Command Reference (2013), at 252
		
		shutdown (OSPFv2)
		The shutdown command disables OSPFv2 on the switch. Neighbor routers are notified of the shutdown and all traffic that has another path through the network will be directed to an alternate path.
		OSPFv2 is disabled on individual interfaces with the shutdown (OSPFv2) command.
		The **no shutdown** and **default shutdown** commands enable the OSPFv2 instance by removing the **shutdown** statement from the OSPF block in *running-config*.
		Platform all
		Command Mode Router-OSPF Configuration
		Command Syntax
		`shutdown`
		`no shutdown`
		`default shutdown`
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1468
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1253; Arista User Manual, v. 4.11.1 (1/11/13), at 1005; Arista User Manual v. 4.10.3 (10/22/12), at 834; Arista User Manual v. 4.9.3.2 (5/3/12), at 658; Arista User Manual v. 4.8.2 (11/18/11), at 493; Arista User Manual v. 4.7.3 (7/18/11), at 365; Arista User Manual v. 4.6.0 (12/22/2010), at 224

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 timers lsa arrival To set the minimum interval at which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the **timers lsa arrival**command in router configuration mode. To restore the default value, use the **no** form of this command. **timers lsa arrival** *milliseconds* **no timers lsa arrival** Syntax Description *milliseconds* Minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is from 0 to 600,000 milliseconds. The default is 1000 milliseconds. Cisco IOS IP Routing:OSPF Command Reference (2013), at 286.	 timers lsa arrival (OSPFv2) The **timers lsa arrival** command sets the minimum interval in which the switch accepts the same link-state advertisement (LSA) from OSPF) neighbors. The **no timers lsa arrival** and **default timers lsa arrival** commands restore the default maximum OSPFv2 path calculation interval to five seconds by removing the **timers lsa arrival** command from *running-config*. Platform all Command Mode Router-OSPF Configuration Command Syntax **timers lsa arrival** *lsa_time* **no timers lsa arrival** **default timers lsa arrival** Parameters • *lsa_time* OSPFv2 mnimum interval (seconds). Values range from 1 to 600000 milliseconds. Default is 1000 milliseconds. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1469.

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	
	timers basic (RIP)
	To adjust Routing Information Protocol (RIP) network timers, use the **timers basic** command in router configuration mode. To restore the default timers, use the **no** form of this command.
	timers basic *update invalid holddown flush*
	no timers basic
	Syntax Description
	update — Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.
	invalid — Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update*argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a *holddown* state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.
	
	Cisco IOS IP Routing:RIP Command Reference (2013), at 56.
		
		timers basic (RIP)
		The **timers basic** command configures the update interval, the expiration time, and the deletion time for routes received and sent through RIP. The command requires value declaration of all values.
		• The update time is the interval between unsolicited route responses. The default is 30 seconds.
		• The expiration time is initialized when a route is established and any time an update is received for the route. If the specified period elapses from the last time the route update was received, then the route is marked as inaccessible and advertised as unreachable. However, the route forwards packets until the deletion time expires. The default value is 180 seconds.
		• The deletion time is initialized when the expiration time has elapsed. On initialization of the deletion time, the route is no longer valid; however, it is retained in the routing table for a short time so that neighbors can be notified that the route has been dropped. Upon expiration of the deletion time, the route is removed from the routing table. The default is 120 seconds.
		The **no timers basic** and **default timers basic** commands return the timer values to their default values by removing the **timers-basic** command from *running-config*.
		Platform all
		Command Mode Router-RIP Configuration
		Command Syntax
		`timers basic` *`update_time expire_time deletion_time`*
		`no timers basic`
		`default timers basic`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1671.
		
		See also Arista User Manual v. 4.13.6F (4/14/2014), at 1621; Arista User Manual v. 4.12.3 (7/17/13), at 1433; Arista User Manual, v. 4.11.1 (1/11/13), at 1179; Arista User Manual v. 4.10.3 (10/22/12), at 989; Arista User Manual v. 4.9.3.2 (5/3/12), at 748; Arista User Manual v. 4.8.2 (11/18/11), at 570.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4
Effective date of registration: 11/26/2014</td>
<td>


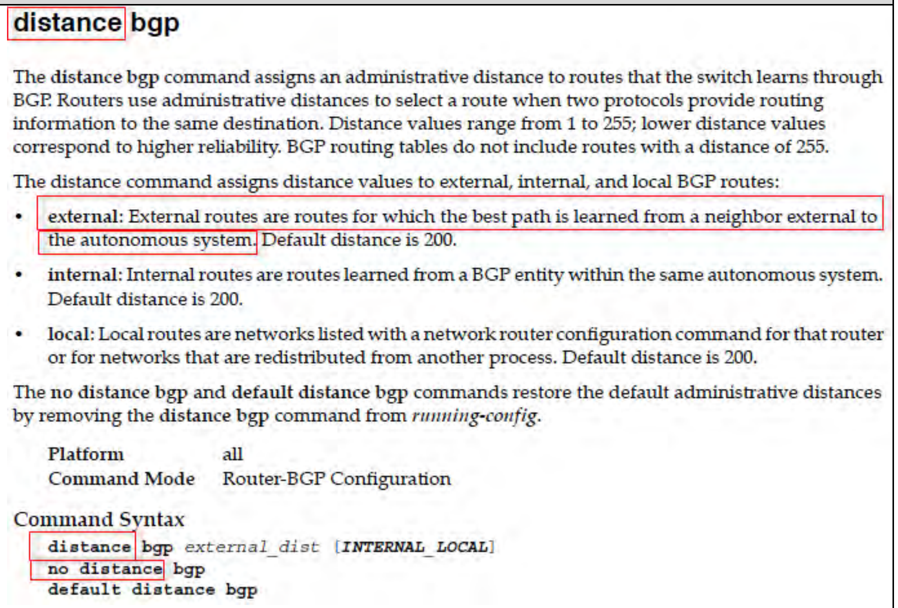
distance (IPv6 EIGRP)

To allow the use of two administrative distances--internal and external--that could be a better route to a node, use the <b>distance</b>command in router configuration mode. To reset these values to their defaults, use the <b>no</b> form of this command.

<b>distance</b> <i>internal-distance external-distance</i>
<b>no distance</b>

Syntax Description

<table>
<tr><td><i>internal-distance</i></td><td>Administrative distance for Enhanced Internal Gateway Routing Protocol (EIGRP) for IPv6 internal routes. Internal routes are those that are learned from another entity within the same autonomous system. The distance can be a value from 1 to 255.</td></tr>
<tr><td><i>external-distance</i></td><td>Administrative distance for EIGRP for IPv6 external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. The distance can be a value from 1 to 255.</td></tr>
</table>

Cisco IOS IP Routing: EIGRP Command Reference (2013), at 42.
</td>
<td>


distance bgp

The <b>distance bgp</b> command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.

The distance command assigns distance values to external, internal, and local BGP routes:

- <b>external</b>: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.
- <b>internal</b>: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.
- <b>local</b>: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200.

The <b>no distance bgp</b> and <b>default distance bgp</b> commands restore the default administrative distances by removing the <b>distance bgp</b> command from <i>running-config</i>.

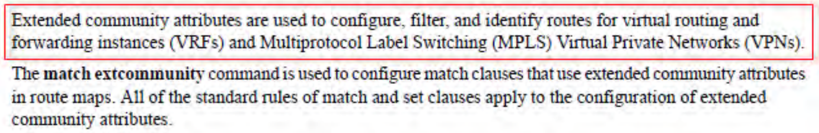
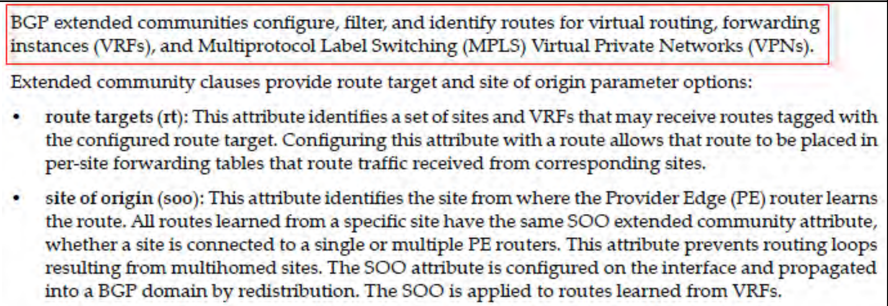
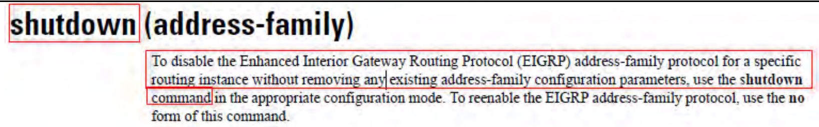
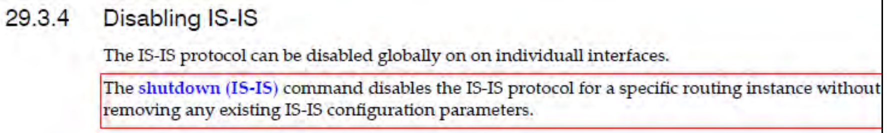
Platform all
Command Mode Router-BGP Configuration

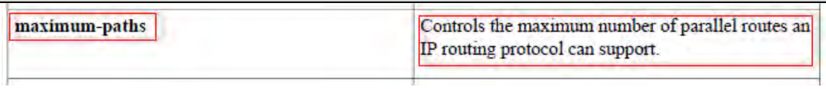
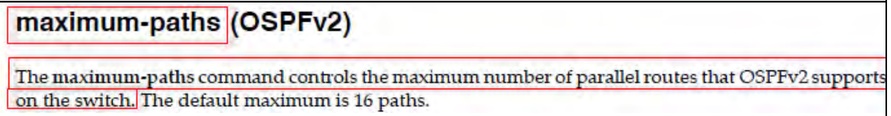
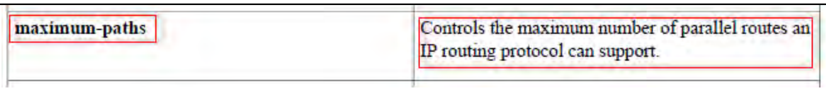
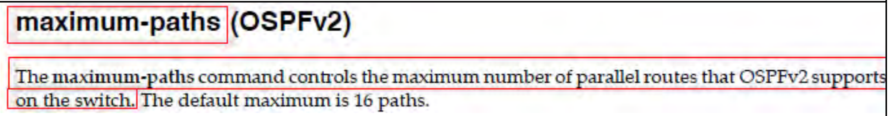
Command Syntax

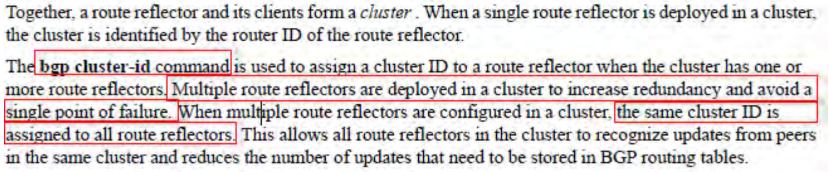
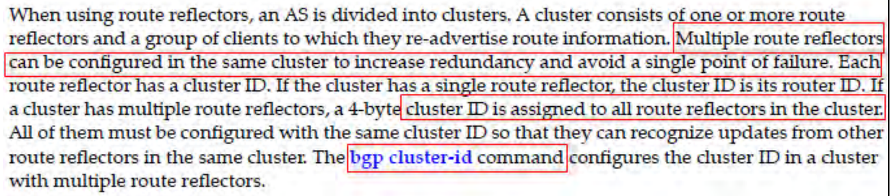
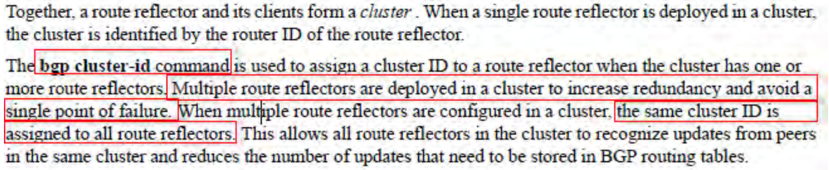
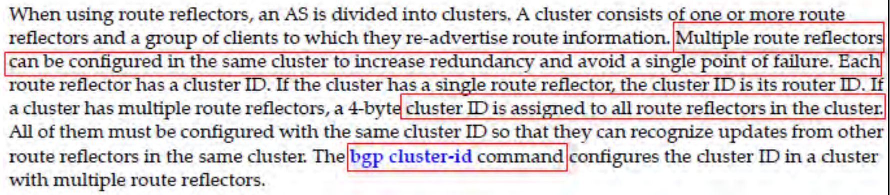
```
distance bgp external_dist [INTERNAL_LOCAL]
no distance bgp
default distance bgp
```

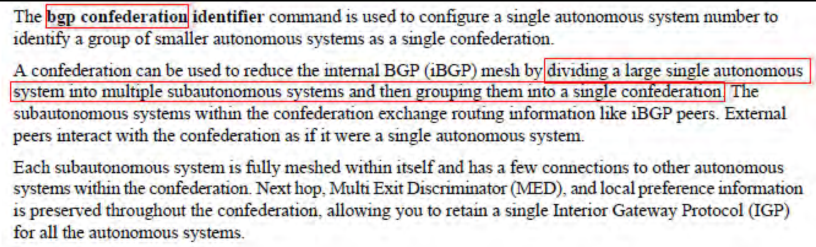
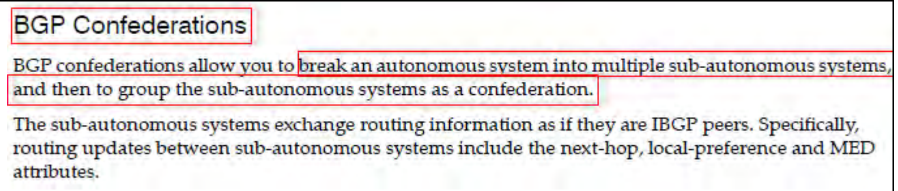
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1583.

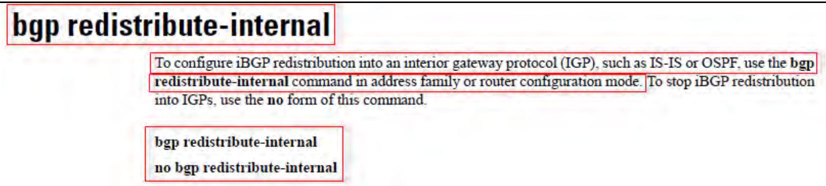
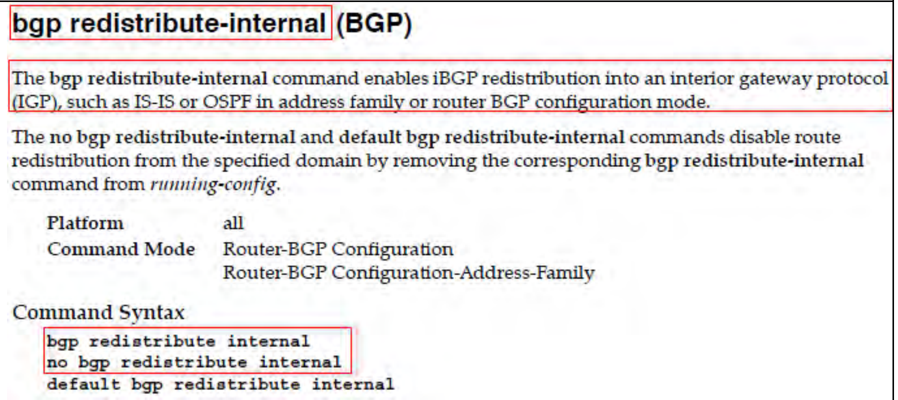
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.
</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). The **match extcommunity** command is used to configure match clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes. Cisco IOS IP Routing: EIGRP Command Reference (2013), at 130.	 BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Extended community clauses provide route target and site of origin parameter options: • **route targets (rt):** This attribute identifies a set of sites and VRFs that may receive routes tagged with the configured route target. Configuring this attribute with a route allows that route to be placed in per-site forwarding tables that route traffic received from corresponding sites. • **site of origin (soo):** This attribute identifies the site from where the Provider Edge (PE) router learns the route. All routes learned from a specific site have the same SOO extended community attribute, whether a site is connected to a single or multiple PE routers. This attribute prevents routing loops resulting from multihomed sites. The SOO attribute is configured on the interface and propagated into a BGP domain by redistribution. The SOO is applied to routes learned from VRFs. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1552. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 at 500.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **shutdown (address-family)** To disable the Enhanced Interior Gateway Routing Protocol (EIGRP) address-family protocol for a specific routing instance without removing any existing address-family configuration parameters, use the **shutdown** command in the appropriate configuration mode. To reenable the EIGRP address-family protocol, use the **no** form of this command. Cisco IOS IP Routing: EIGRP Command Reference (2013), at 276.	 29.3.4 Disabling IS-IS The IS-IS protocol can be disabled globally on on individuall interfaces. The **shutdown (IS-IS)** command disables the IS-IS protocol for a specific routing instance without removing any existing IS-IS configuration parameters. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1679. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1440.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 maximum-paths Controls the maximum number of parallel routes an IP routing protocol can support. Cisco IOS IP Routing: BGP Command Reference (2013), at 375.	 maximum-paths (OSPFv2) The maximum-paths command controls the maximum number of parallel routes that OSPFv2 supports on the switch. The default maximum is 16 paths. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1440. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1226; Arista User Manual, v. 4.11.1 (1/11/13), at 983; Arista User Manual v. 4.10.3 (10/22/12), at 813; Arista User Manual v. 4.9.3.2 (5/3/12), at 637; Arista User Manual v. 4.8.2 (11/18/11), at 472.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 maximum-paths Controls the maximum number of parallel routes an IP routing protocol can support. Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 146.	 maximum-paths (OSPFv2) The maximum-paths command controls the maximum number of parallel routes that OSPFv2 supports on the switch. The default maximum is 16 paths. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1440. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1226; Arista User Manual, v. 4.11.1 (1/11/13), at 983; Arista User Manual v. 4.10.3 (10/22/12), at 813; Arista User Manual v. 4.9.3.2 (5/3/12), at 637; Arista User Manual v. 4.8.2 (11/18/11), at 472.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 Together, a route reflector and its clients form a *cluster* . When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector. The **bgp cluster-id** command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables. Cisco IOS IP Routing: BGP Command Reference (2013), at 74.	 When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. Multiple route reflectors can be configured in the same cluster to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The **bgp cluster-id** command configures the cluster ID in a cluster with multiple route reflectors. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1549. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1331; Arista User Manual, v. 4.11.1 (1/11/13), at 1081; Arista User Manual v. 4.10.3 (10/22/12), at 893; Arista User Manual v. 4.9.3.2 (5/3/12), at 665.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 Together, a route reflector and its clients form a *cluster* . When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector. The **bgp cluster-id** command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables. Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 25.	 When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. Multiple route reflectors can be configured in the same cluster to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The **bgp cluster-id** command configures the cluster ID in a cluster with multiple route reflectors. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1549. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1331; Arista User Manual, v. 4.11.1 (1/11/13), at 1081; Arista User Manual v. 4.10.3 (10/22/12), at 893; Arista User Manual v. 4.9.3.2 (5/3/12), at 665.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 The **bgp confederation identifier** command is used to configure a single autonomous system number to identify a group of smaller autonomous systems as a single confederation. A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. The subautonomous systems within the confederation exchange routing information like iBGP peers. External peers interact with the confederation as if it were a single autonomous system. Each subautonomous system is fully meshed within itself and has a few connections to other autonomous systems within the confederation. Next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems. Cisco IOS IP Routing: BGP Command Reference (2013), at 77	 BGP Confederations BGP confederations allow you to break an autonomous system into multiple sub-autonomous systems, and then to group the sub-autonomous systems as a confederation. The sub-autonomous systems exchange routing information as if they are IBGP peers. Specifically, routing updates between sub-autonomous systems include the next-hop, local-preference and MED attributes. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1556. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1326.

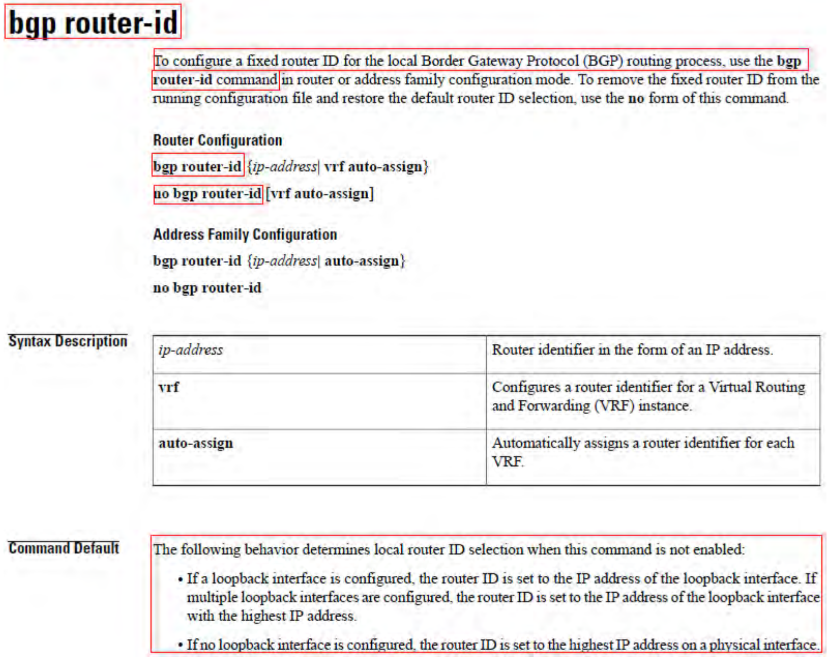
Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	bgp redistribute-internal
	To configure iBGP redistribution into an interior gateway protocol (IGP), such as IS-IS or OSPF, use the **bgp redistribute-internal** command in address family or router configuration mode. To stop iBGP redistribution into IGPs, use the **no** form of this command.
	bgp redistribute-internal
	no bgp redistribute-internal
	Cisco IOS IP Routing: BGP Command Reference (2013), at 133
		
		bgp redistribute-internal (BGP)
		The **bgp redistribute-internal** command enables iBGP redistribution into an interior gateway protocol (IGP), such as IS-IS or OSPF in address family or router BGP configuration mode.
		The **no bgp redistribute-internal** and **default bgp redistribute-internal** commands disable route redistribution from the specified domain by removing the corresponding **bgp redistribute-internal** command from *running-config*.
		Platform all
		Command Mode Router-BGP Configuration
		Router-BGP Configuration-Address-Family
		Command Syntax
		`bgp redistribute internal`
		`no bgp redistribute internal`
		`default bgp redistribute internal`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1576.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1357.

<table>
<tr>
<th>Copyright Registration Information</th>
<th>Cisco</th>
<th>Arista</th>
</tr>
<tr>
<td>

Cisco IOS 15.4

Effective date of registration: 11/26/2014

</td>
<td>



bgp router-id

To configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process, use the **bgp router-id** command in router or address family configuration mode. To remove the fixed router ID from the running configuration file and restore the default router ID selection, use the **no** form of this command.

Router Configuration

bgp router-id {*ip-address*| **vrf auto-assign**}

no bgp router-id [**vrf auto-assign**]

Address Family Configuration

bgp router-id {*ip-address*| **auto-assign**}

no bgp router-id

Syntax Description

<table>
<tr><td><i>ip-address</i></td><td>Router identifier in the form of an IP address.</td></tr>
<tr><td><b>vrf</b></td><td>Configures a router identifier for a Virtual Routing and Forwarding (VRF) instance.</td></tr>
<tr><td><b>auto-assign</b></td><td>Automatically assigns a router identifier for each VRF.</td></tr>
</table>

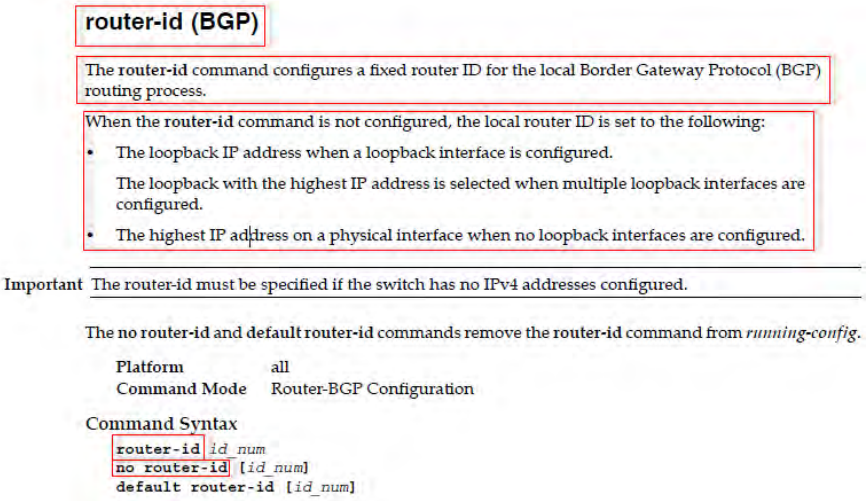
Command Default

The following behavior determines local router ID selection when this command is not enabled:

- If a loopback interface is configured, the router ID is set to the IP address of the loopback interface. If multiple loopback interfaces are configured, the router ID is set to the IP address of the loopback interface with the highest IP address.
- If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.

Cisco IOS IP Routing: BGP Command Reference (2013), at 142.

</td>
<td>



router-id (BGP)

The **router-id** command configures a fixed router ID for the local Border Gateway Protocol (BGP) routing process.

When the **router-id** command is not configured, the local router ID is set to the following:

- The loopback IP address when a loopback interface is configured.

  The loopback with the highest IP address is selected when multiple loopback interfaces are configured.
- The highest IP address on a physical interface when no loopback interfaces are configured.

Important The router-id must be specified if the switch has no IPv4 addresses configured.

The **no router-id** and **default router-id** commands remove the **router-id** command from *running-config*.

Platform all
Command Mode Router-BGP Configuration

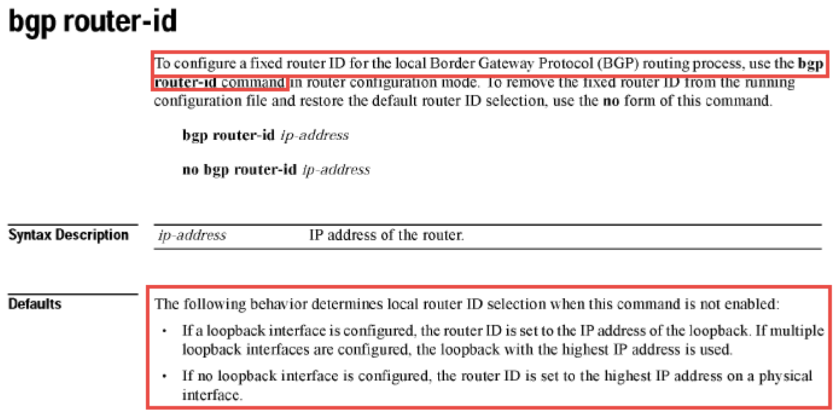
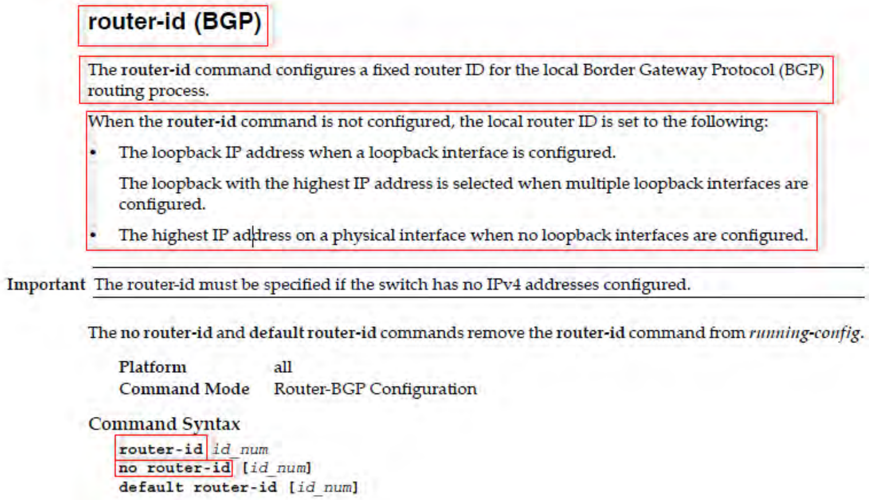
Command Syntax

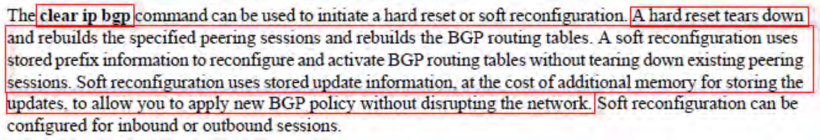
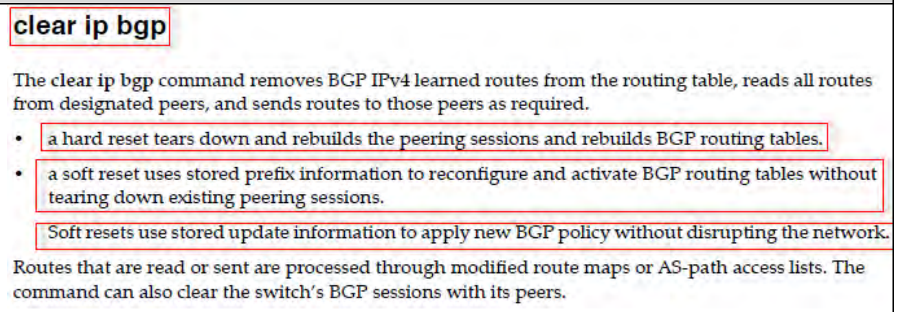
```
router-id id_num
no router-id [id_num]
default router-id [id_num]
```

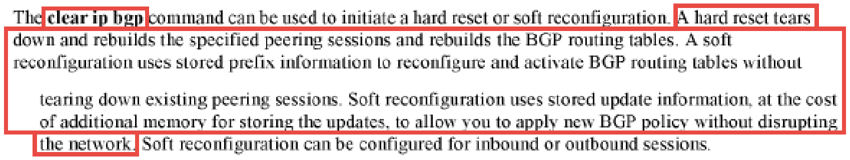
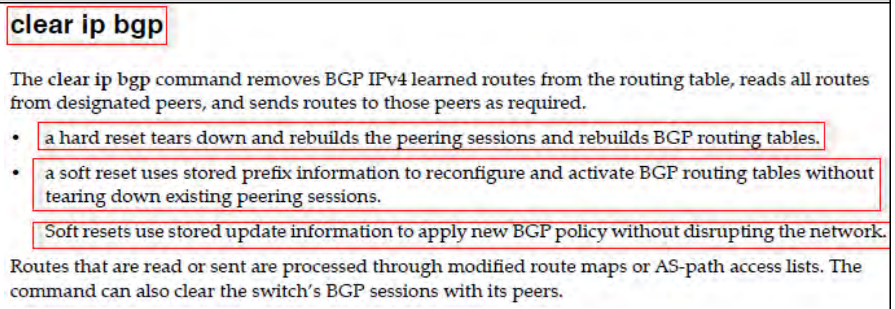
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1625.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1397; Arista User Manual, v. 4.11.1 (1/11/13), at 1143; Arista User Manual v. 4.10.3 (10/22/12), at 954; Arista User Manual v. 4.9.3.2 (5/3/12), at 716.

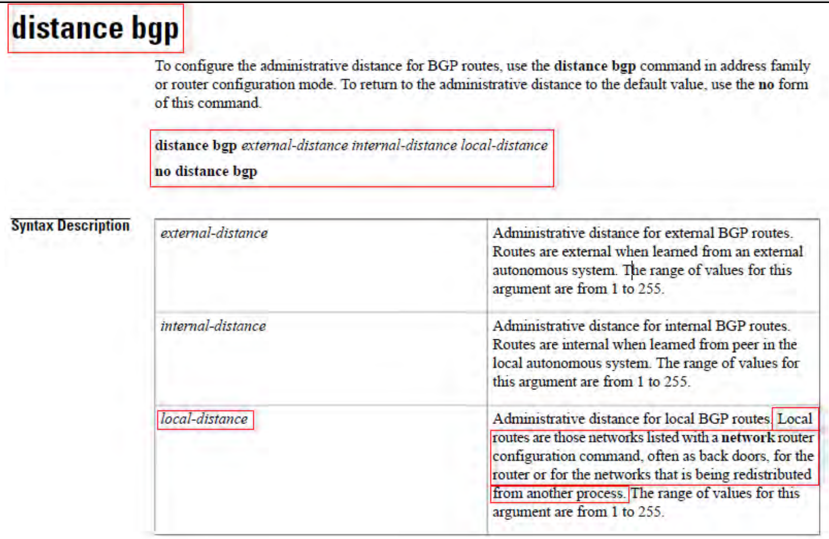
</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 **bgp router-id** To configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process, use the **bgp router-id** command in router configuration mode. To remove the fixed router ID from the running configuration file and restore the default router ID selection, use the **no** form of this command. **bgp router-id** *ip-address* **no bgp router-id** *ip-address* **Syntax Description** — *ip-address* IP address of the router. **Defaults** — The following behavior determines local router ID selection when this command is not enabled: • If a loopback interface is configured, the router ID is set to the IP address of the loopback. If multiple loopback interfaces are configured, the loopback with the highest IP address is used. • If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface. Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 55.	 **router-id (BGP)** The **router-id** command configures a fixed router ID for the local Border Gateway Protocol (BGP) routing process. When the **router-id** command is not configured, the local router ID is set to the following: • The loopback IP address when a loopback interface is configured. The loopback with the highest IP address is selected when multiple loopback interfaces are configured. • The highest IP address on a physical interface when no loopback interfaces are configured. **Important** The router-id must be specified if the switch has no IPv4 addresses configured. The **no router-id** and **default router-id** commands remove the **router-id** command from *running-config*. **Platform** all **Command Mode** Router-BGP Configuration Command Syntax `router-id` *id_num* `no router-id` [*id_num*] `default router-id` [*id_num*] Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1625. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1397; Arista User Manual, v. 4.11.1 (1/11/13), at 1143; Arista User Manual v. 4.10.3 (10/22/12), at 954; Arista User Manual v. 4.9.3.2 (5/3/12), at 716.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 The **clear ip bgp** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions. Cisco IOS IP Routing: BGP Command Reference (2013), at 193	 **clear ip bgp** The **clear ip bgp** command removes BGP IPv4 learned routes from the routing table, reads all routes from designated peers, and sends routes to those peers as required. • a hard reset tears down and rebuilds the peering sessions and rebuilds BGP routing tables. • a soft reset uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft resets use stored update information to apply new BGP policy without disrupting the network. Routes that are read or sent are processed through modified route maps or AS-path access lists. The command can also clear the switch's BGP sessions with its peers. Arista User Manual v. 4.14.3F (Rev. 2) 10/2/2014), at 1577. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1527; Arista User Manual v. 4.12.3 (7/17/13), at 1358; Arista User Manual, v. 4.11.1 (1/11/13), at 1104; Arista User Manual v. 4.10.3 (10/22/12), at 916; Arista User Manual v. 4.9.3.2 (5/3/12), at 683; Arista User Manual v. 4.8.2 (11/18/11), at 513; Arista User Manual v. 4.7.3 (7/18/11), at 378.

Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 The **clear ip bgp** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions. Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 72-73.	 **clear ip bgp** The clear ip bgp command removes BGP IPv4 learned routes from the routing table, reads all routes from designated peers, and sends routes to those peers as required. • a hard reset tears down and rebuilds the peering sessions and rebuilds BGP routing tables. • a soft reset uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft resets use stored update information to apply new BGP policy without disrupting the network. Routes that are read or sent are processed through modified route maps or AS-path access lists. The command can also clear the switch's BGP sessions with its peers. Arista User Manual v. 4.14.3F (Rev. 2) 10/2/2014), at 1577. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1527; Arista User Manual v. 4.12.3 (7/17/13), at 1358; Arista User Manual, v. 4.11.1 (1/11/13), at 1104; Arista User Manual v. 4.10.3 (10/22/12), at 916; Arista User Manual v. 4.9.3.2 (5/3/12), at 683; Arista User Manual v. 4.8.2 (11/18/11), at 513; Arista User Manual v. 4.7.3 (7/18/11), at 378.

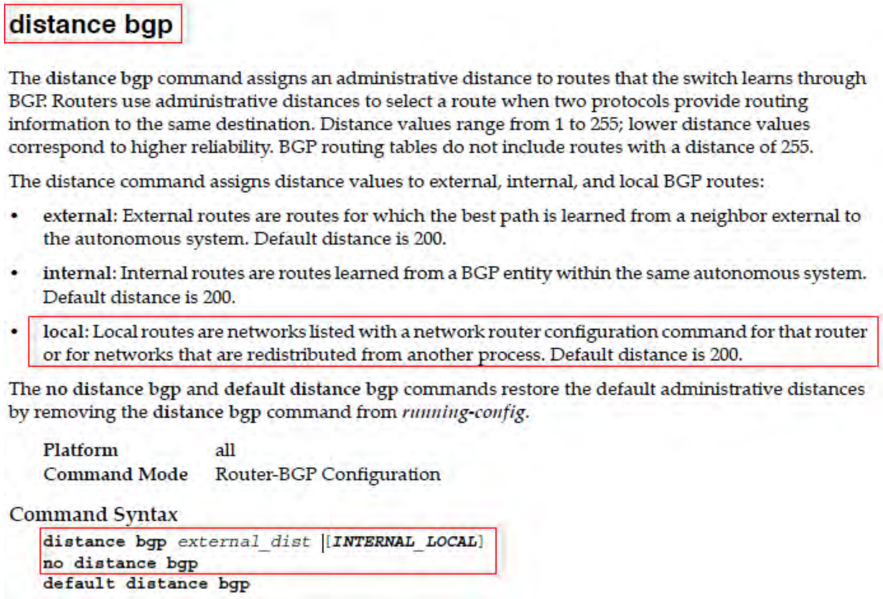
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>

<b>distance bgp</b>

To configure the administrative distance for BGP routes, use the <b>distance bgp</b> command in address family or router configuration mode. To return to the administrative distance to the default value, use the <b>no</b> form of this command.

<b>distance bgp</b> <i>external-distance internal-distance local-distance</i>
<b>no distance bgp</b>

<b>Syntax Description</b>
<table>
<tr><td><i>external-distance</i></td><td>Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.</td></tr>
<tr><td><i>internal-distance</i></td><td>Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.</td></tr>
<tr><td><i>local-distance</i></td><td>Administrative distance for local BGP routes. Local routes are those networks listed with a <b>network</b> router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.</td></tr>
</table>

Cisco IOS IP Routing: BGP Command Reference (2013), at 271.
</td>
<td>

<b>distance bgp</b>

The <b>distance bgp</b> command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.

The distance command assigns distance values to external, internal, and local BGP routes:
• <b>external</b>: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.
• <b>internal</b>: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.
• <b>local</b>: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200.

The <b>no distance bgp</b> and <b>default distance bgp</b> commands restore the default administrative distances by removing the <b>distance bgp</b> command from <i>running-config</i>.

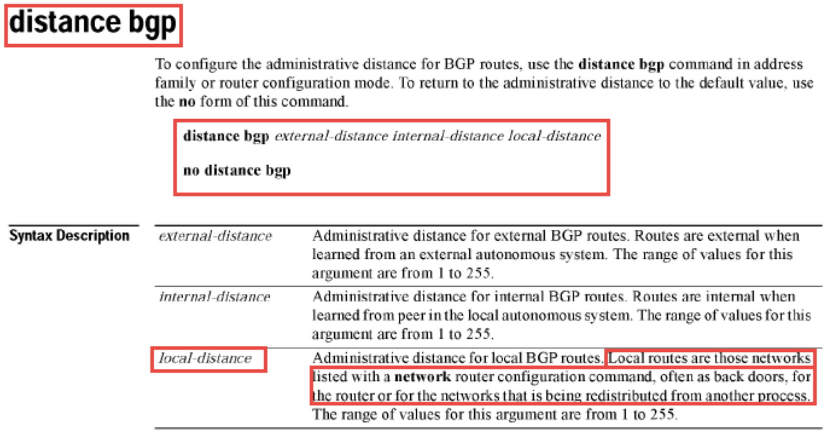
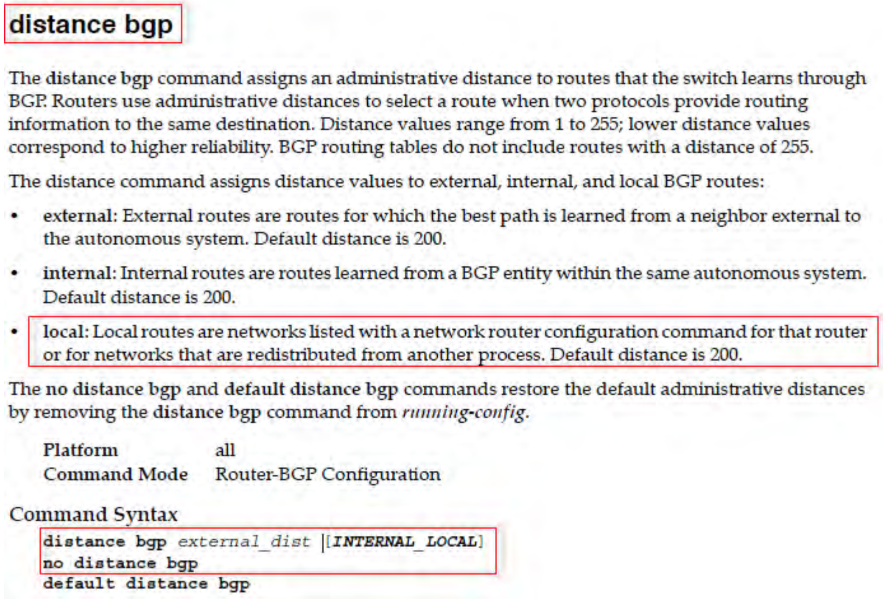
Platform all
Command Mode Router-BGP Configuration

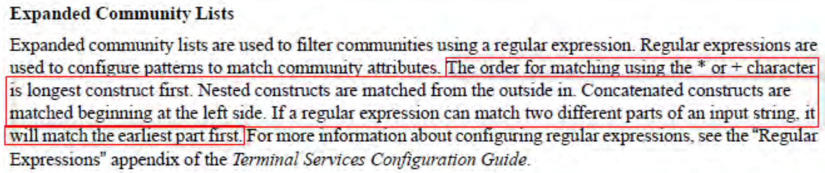
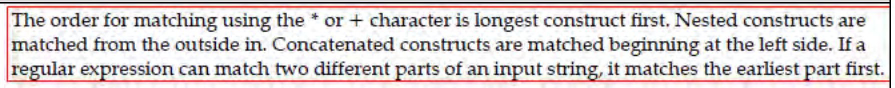
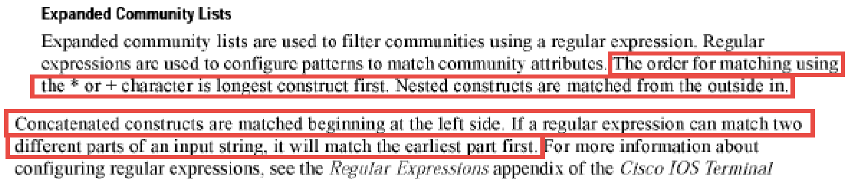
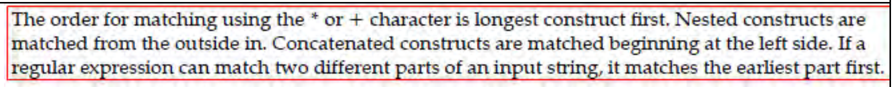
Command Syntax
<code>distance bgp <i>external_dist</i> |[<i>INTERNAL_LOCAL</i>]</code>
<code>no distance bgp</code>
<code>default distance bgp</code>

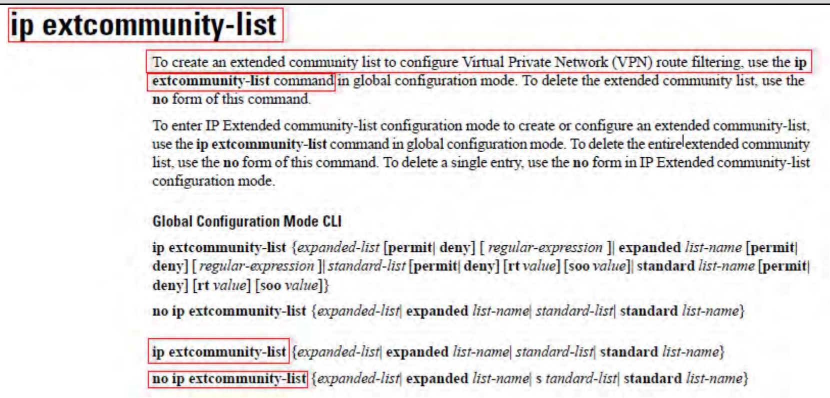
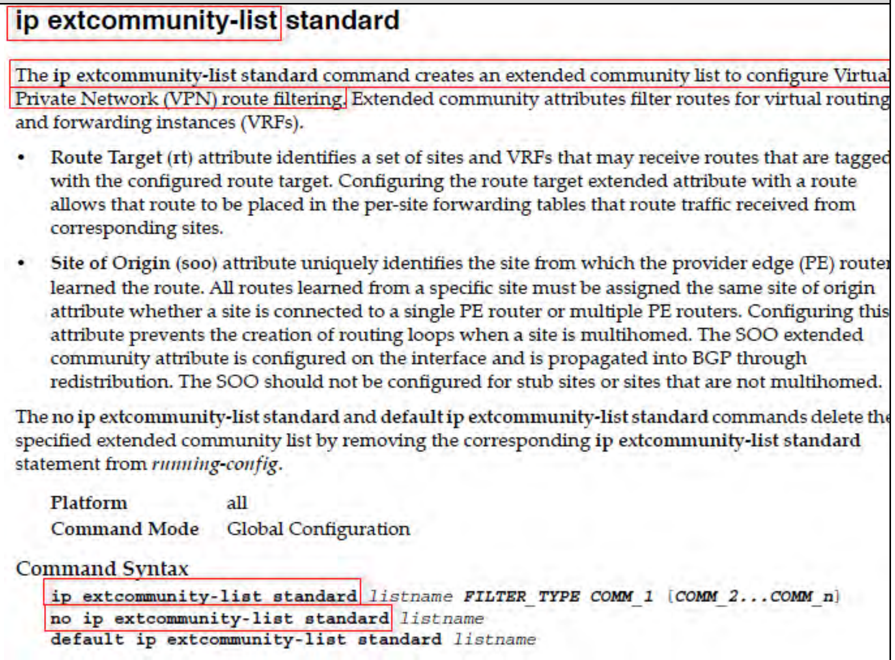
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1583.

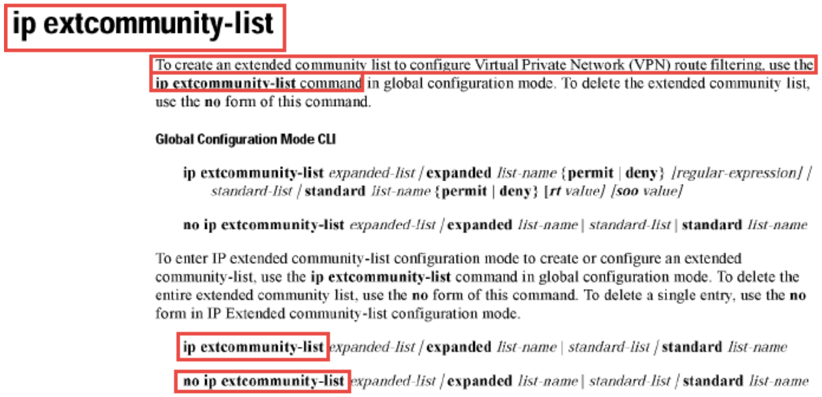
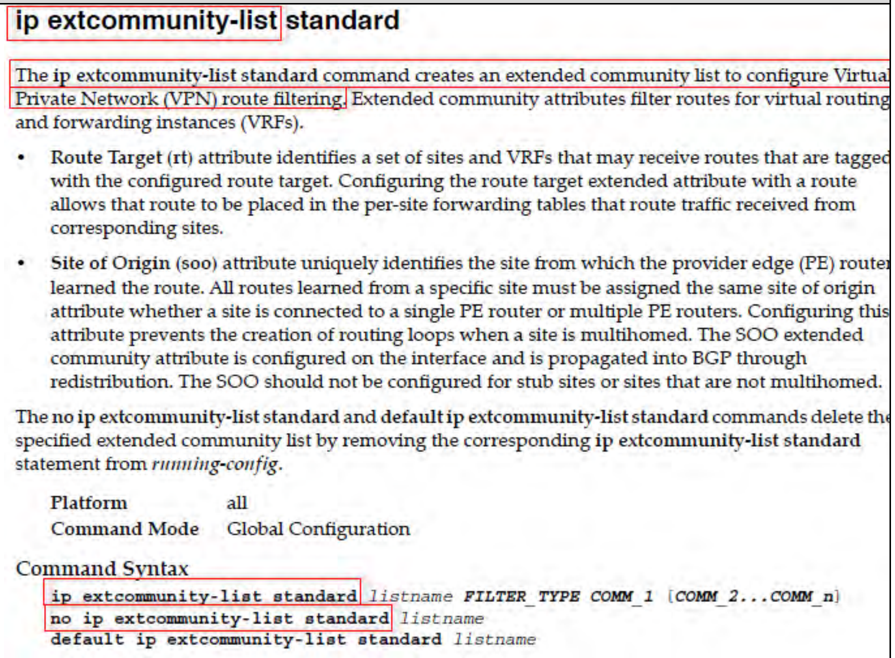
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.
</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista

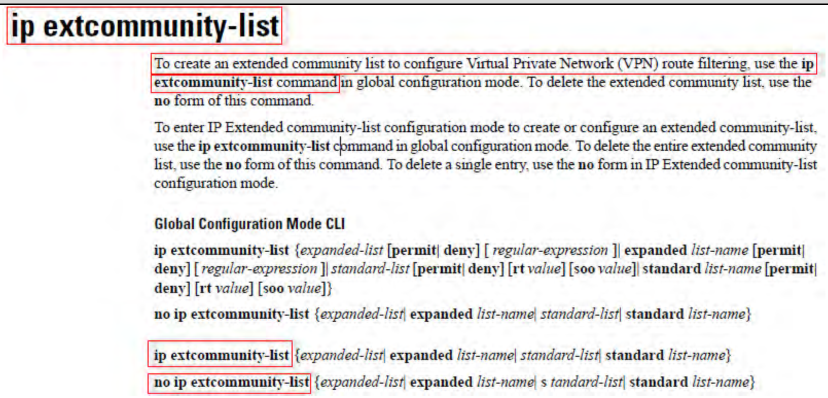
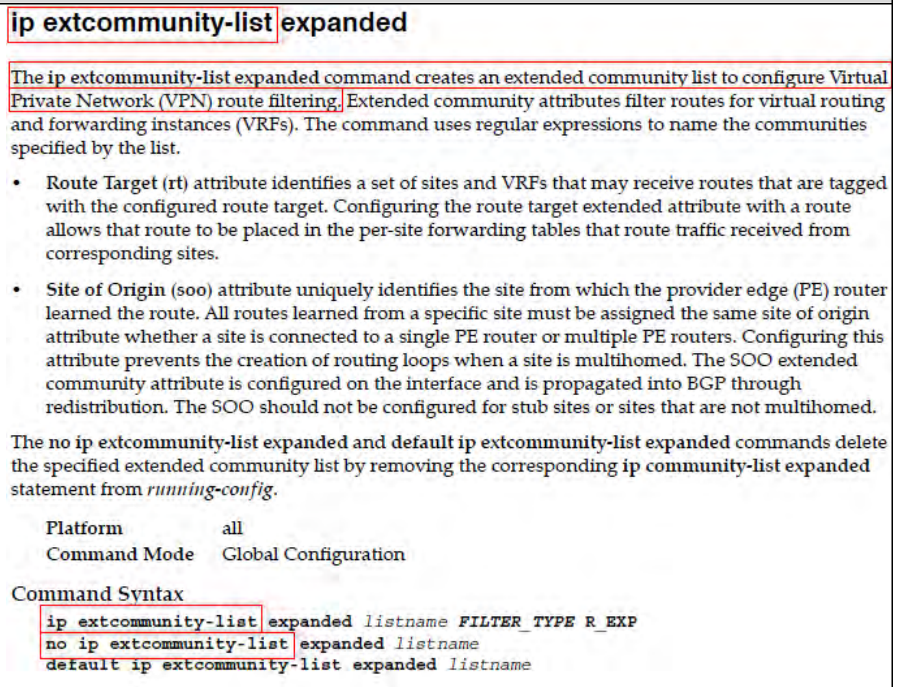
Cisco IOS 12.4
Effective date of registration: 8/12/2005
	
	distance bgp
	To configure the administrative distance for BGP routes, use the **distance bgp** command in address family or router configuration mode. To return to the administrative distance to the default value, use the **no** form of this command.
	distance bgp *external-distance internal-distance local-distance*
	no distance bgp
	Syntax Description
	external-distance Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.
	internal-distance Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.
	local-distance Administrative distance for local BGP routes. Local routes are those networks listed with a **network** router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.
	Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 95.
		
		distance bgp
		The **distance bgp** command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.
		The distance command assigns distance values to external, internal, and local BGP routes:
		• **external**: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.
		• **internal**: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.
		• **local**: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200.
		The **no distance bgp** and **default distance bgp** commands restore the default administrative distances by removing the **distance bgp** command from *running-config*.
		Platform all
		Command Mode Router-BGP Configuration
		Command Syntax
		`distance bgp external_dist |[INTERNAL_LOCAL]`
		`no distance bgp`
		`default distance bgp`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1583.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.

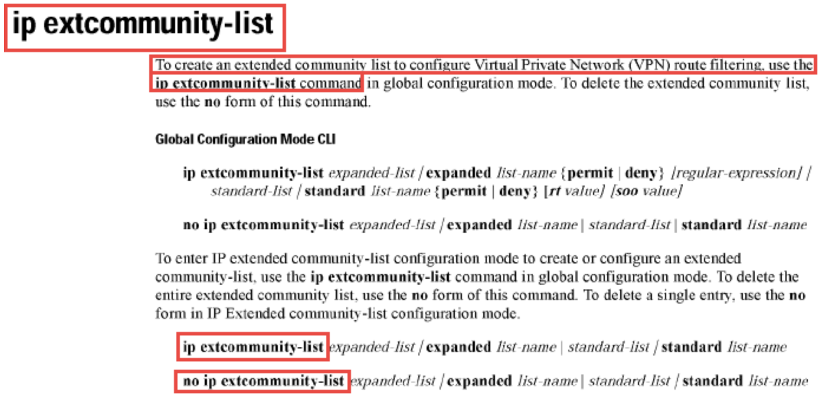
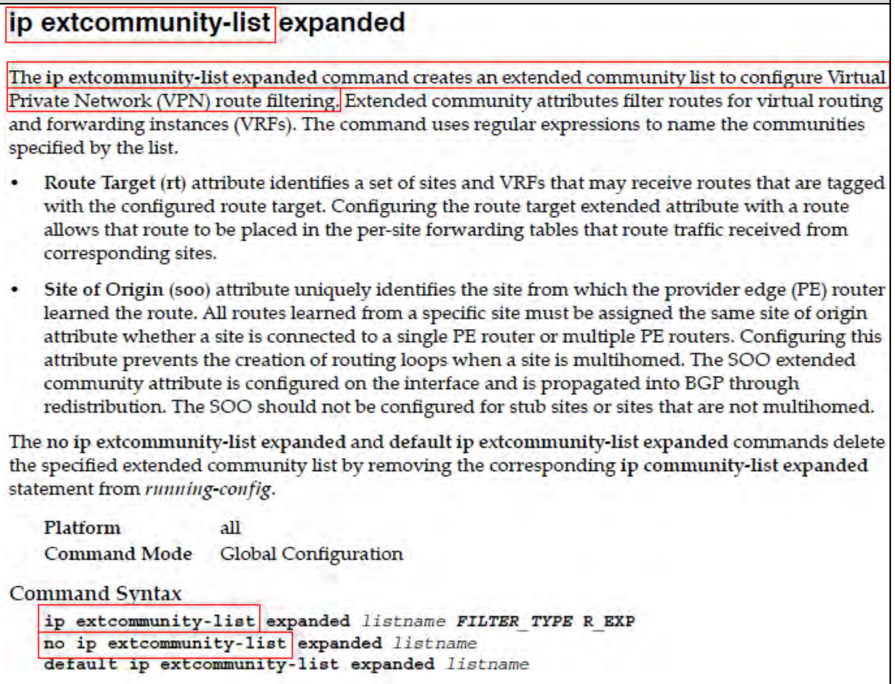
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Expanded Community Lists** Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the "Regular Expressions" appendix of the *Terminal Services Configuration Guide*. Cisco IOS IP Routing: BGP Command Reference (2013), at 324.	 The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 107. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 **Expanded Community Lists** Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the *Regular Expressions* appendix of the *Cisco IOS Terminal* Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 117-18.	 The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 107. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.

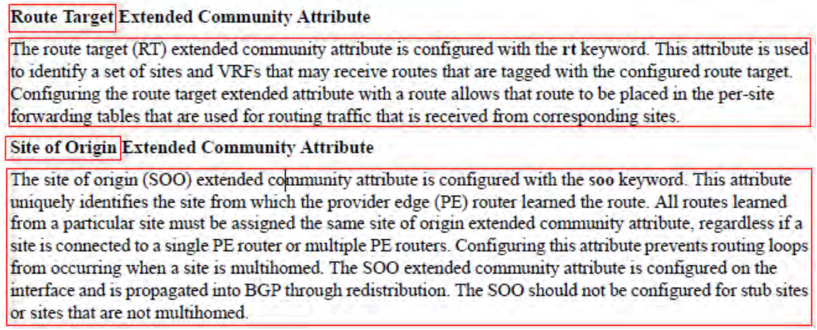
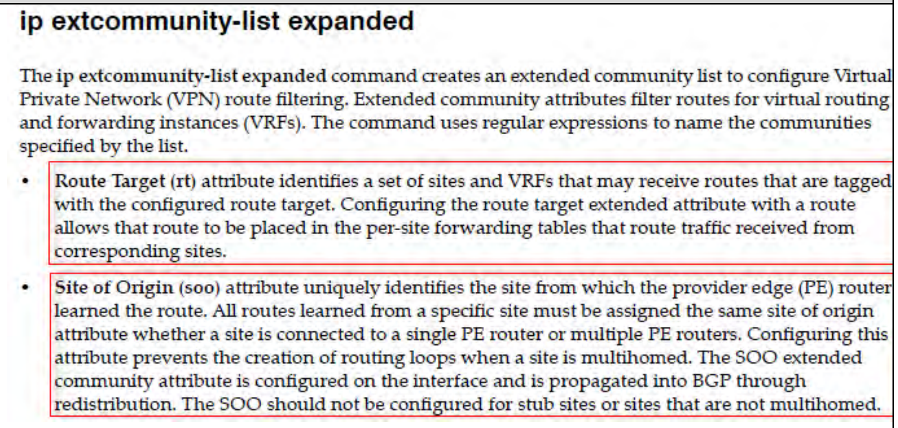
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **ip extcommunity-list** To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the **ip extcommunity-list** command in global configuration mode. To delete the extended community list, use the **no** form of this command. To enter IP Extended community-list configuration mode to create or configure an extended community-list, use the **ip extcommunity-list** command in global configuration mode. To delete the entire extended community list, use the **no** form of this command. To delete a single entry, use the **no** form in IP Extended community-list configuration mode. **Global Configuration Mode CLI** **ip extcommunity-list** {*expanded-list* [**permit**| **deny**] [*regular-expression*]| **expanded** *list-name* [**permit**| **deny**] [*regular-expression*]| *standard-list* [**permit**| **deny**] [**rt** *value*] [**soo** *value*]| **standard** *list-name* [**permit**| **deny**] [**rt** *value*] [**soo** *value*]} **no ip extcommunity-list** {*expanded-list*| **expanded** *list-name*| *standard-list*| **standard** *list-name*} **ip extcommunity-list** {*expanded-list*| **expanded** *list-name*| *standard-list*| **standard** *list-name*} **no ip extcommunity-list** {*expanded-list*| **expanded** *list-name*| s *tandard-list*| **standard** *list-name*} Cisco IOS IP Routing: BGP Command Reference (2013), at 326	 **ip extcommunity-list standard** The **ip extcommunity-list standard** command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). • Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. The **no ip extcommunity-list standard** and **default ip extcommunity-list standard** commands delete the specified extended community list by removing the corresponding **ip extcommunity-list standard** statement from *running-config*. Platform all Command Mode Global Configuration Command Syntax `ip extcommunity-list standard` *`listname`* ***`FILTER_TYPE COMM_1`*** [***`COMM_2...COMM_n`***] `no ip extcommunity-list standard` *`listname`* `default ip extcommunity-list standard` *`listname`* Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1591. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1541; Arista User Manual v. 4.12.3 (7/17/13), at 1365; Arista User Manual, v. 4.11.1 (1/11/13), at 1111; Arista User Manual v. 4.10.3 (10/22/12), at 923; Arista User Manual v. 4.9.3.2 (5/3/12), at 690; Arista User Manual v. 4.8.2 (11/18/11), at 520.

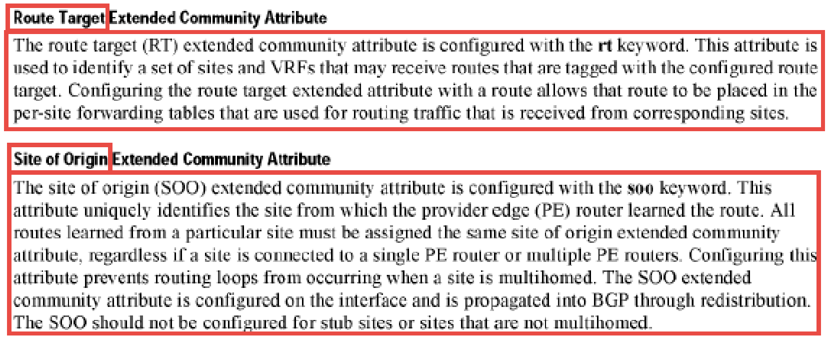
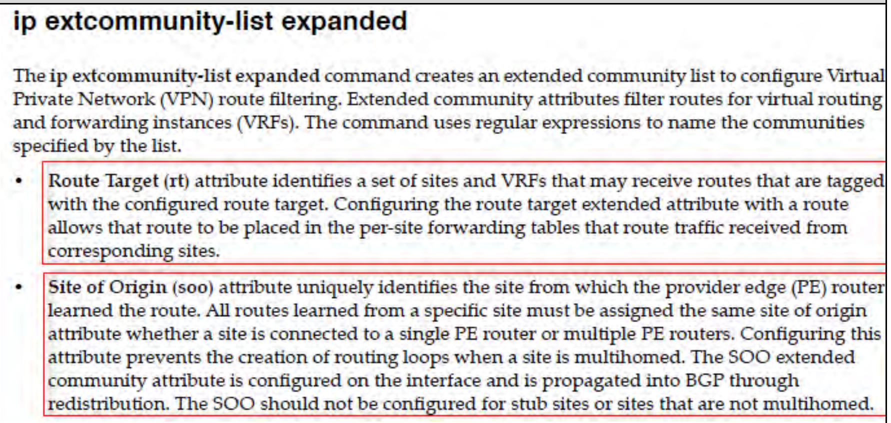
Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 **ip extcommunity-list** To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the **ip extcommunity-list** command in global configuration mode. To delete the extended community list, use the **no** form of this command. **Global Configuration Mode CLI** **ip extcommunity-list** *expanded-list* / **expanded** *list-name* {**permit** | **deny**} *[regular-expression]* / *standard-list* / **standard** *list-name* {**permit** | **deny**} [*rt value*] *[soo value]* **no ip extcommunity-list** *expanded-list* / **expanded** *list-name* | *standard-list* | **standard** *list-name* To enter IP extended community-list configuration mode to create or configure an extended community-list, use the **ip extcommunity-list** command in global configuration mode. To delete the entire extended community list, use the **no** form of this command. To delete a single entry, use the **no** form in IP Extended community-list configuration mode. **ip extcommunity-list** *expanded-list* / **expanded** *list-name* | *standard-list* / **standard** *list-name* **no ip extcommunity-list** *expanded-list* / **expanded** *list-name* | *standard-list* / **standard** *list-name* Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 116.	 **ip extcommunity-list standard** The **ip extcommunity-list standard** command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). • Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. The **no ip extcommunity-list standard** and **default ip extcommunity-list standard** commands delete the specified extended community list by removing the corresponding **ip extcommunity-list standard** statement from *running-config*. Platform all Command Mode Global Configuration Command Syntax `ip extcommunity-list standard` *`listname`* ***`FILTER_TYPE COMM_1`*** [***`COMM_2...COMM_n`***] `no ip extcommunity-list standard` *`listname`* `default ip extcommunity-list standard` *`listname`* Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1591. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1541; Arista User Manual v. 4.12.3 (7/17/13), at 1365; Arista User Manual, v. 4.11.1 (1/11/13), at 1111; Arista User Manual v. 4.10.3 (10/22/12), at 923; Arista User Manual v. 4.9.3.2 (5/3/12), at 690; Arista User Manual v. 4.8.2 (11/18/11), at 520.

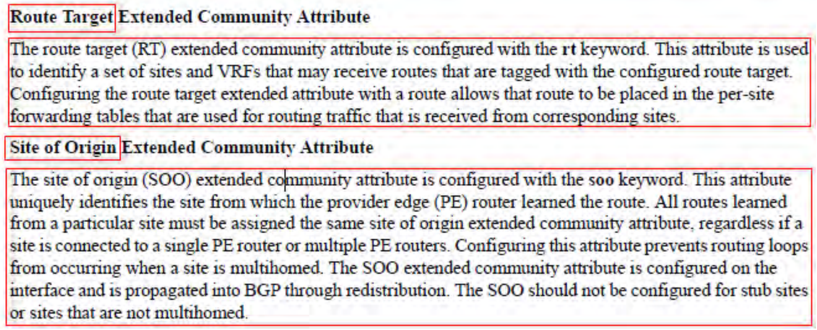
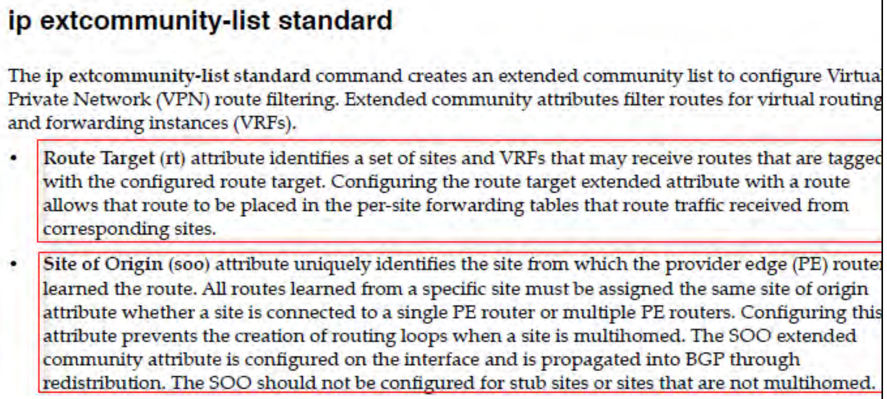
Copyright Registration Information	Cisco	Arista

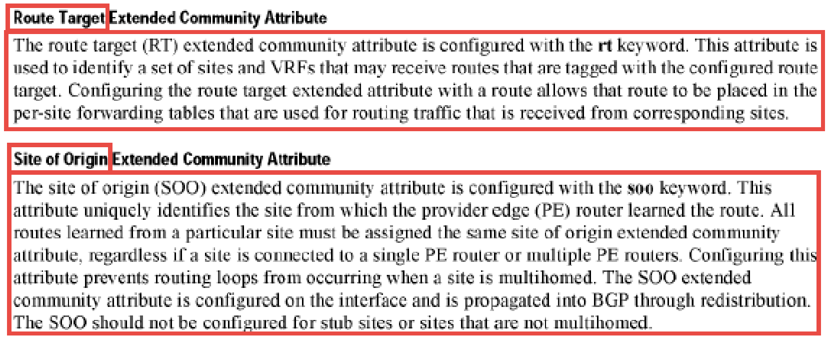
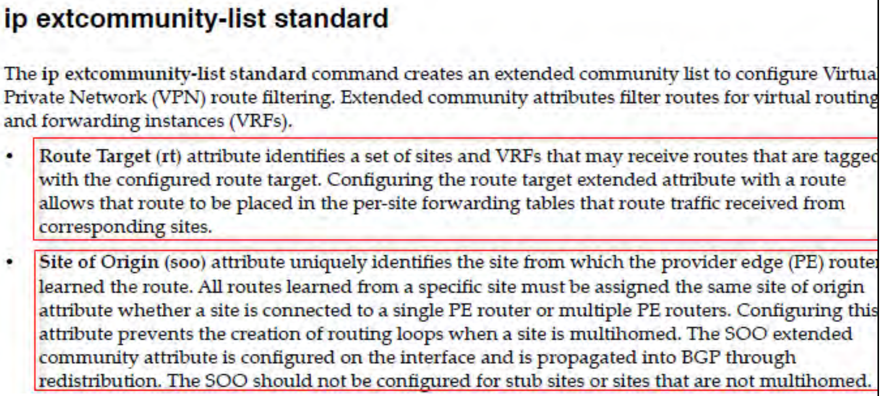
Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	ip extcommunity-list
	To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the **ip extcommunity-list** command in global configuration mode. To delete the extended community list, use the **no** form of this command.
	To enter IP Extended community-list configuration mode to create or configure an extended community-list, use the **ip extcommunity-list** command in global configuration mode. To delete the entire extended community list, use the **no** form of this command. To delete a single entry, use the **no** form in IP Extended community-list configuration mode.
	Global Configuration Mode CLI
	ip extcommunity-list {*expanded-list* [**permit**| **deny**] [*regular-expression*]| **expanded** *list-name* [**permit**| **deny**] [*regular-expression*]| *standard-list* [**permit**| **deny**] [**rt** *value*] [**soo** *value*]| **standard** *list-name* [**permit**| **deny**] [**rt** *value*] [**soo** *value*]}
	no ip extcommunity-list {*expanded-list*| **expanded** *list-name*| *standard-list*| **standard** *list-name*}
	ip extcommunity-list {*expanded-list*| **expanded** *list-name*| *standard-list*| **standard** *list-name*}
	no ip extcommunity-list {*expanded-list*| **expanded** *list-name*| s *tandard-list*| **standard** *list-name*}
	Cisco IOS IP Routing: BGP Command Reference (2013), at 326.
		
		ip extcommunity-list expanded
		The ip extcommunity-list expanded command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list.
		• Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites.
		• Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.
		The **no ip extcommunity-list expanded** and **default ip extcommunity-list expanded** commands delete the specified extended community list by removing the corresponding **ip community-list expanded** statement from *running-config*.
		Platform all
		Command Mode Global Configuration
		Command Syntax
		`ip extcommunity-list expanded listname FILTER_TYPE R_EXP`
		`no ip extcommunity-list expanded listname`
		`default ip extcommunity-list expanded listname`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590.
		See also Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.

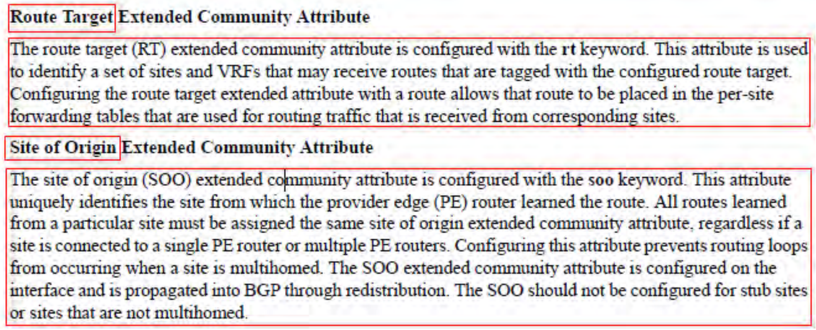
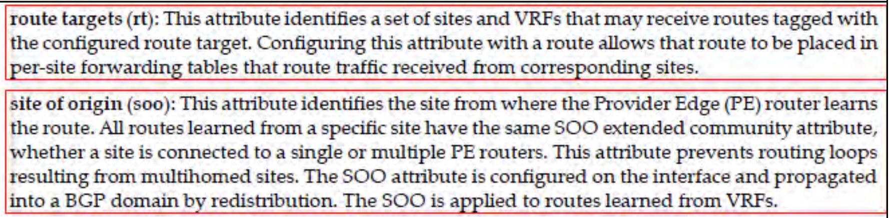
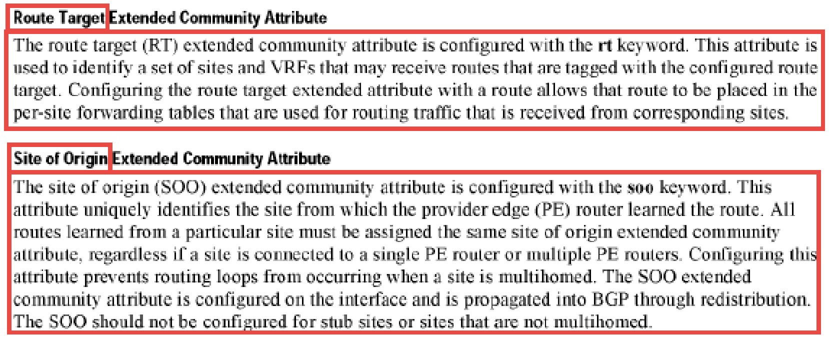
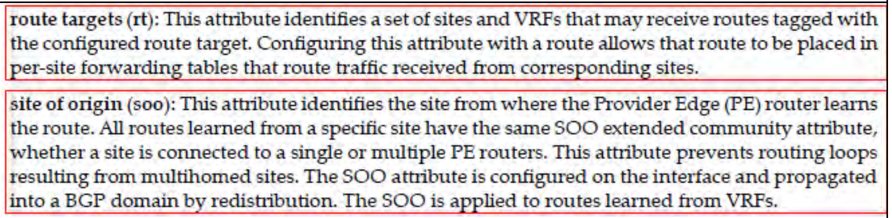
Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 **ip extcommunity-list** To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the **ip extcommunity-list** command in global configuration mode. To delete the extended community list, use the **no** form of this command. **Global Configuration Mode CLI** **ip extcommunity-list** *expanded-list* / **expanded** *list-name* {**permit** | **deny**} *[regular-expression]* / *standard-list* / **standard** *list-name* {**permit** | **deny**} [**rt** *value]* [**soo** *value]* **no ip extcommunity-list** *expanded-list* / **expanded** *list-name* | *standard-list* | **standard** *list-name* To enter IP extended community-list configuration mode to create or configure an extended community-list, use the **ip extcommunity-list** command in global configuration mode. To delete the entire extended community list, use the **no** form of this command. To delete a single entry, use the **no** form in IP Extended community-list configuration mode. **ip extcommunity-list** *expanded-list* / **expanded** *list-name* | *standard-list* / **standard** *list-name* **no ip extcommunity-list** *expanded-list* / **expanded** *list-name* | *standard-list* / **standard** *list-name* Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 116.	 **ip extcommunity-list expanded** The **ip extcommunity-list expanded** command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list. • Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. The **no ip extcommunity-list expanded** and **default ip extcommunity-list expanded** commands delete the specified extended community list by removing the corresponding **ip community-list expanded** statement from *running-config*. Platform all Command Mode Global Configuration Command Syntax **ip extcommunity-list expanded** *listname* ***FILTER_TYPE*** **R_EXP** **no ip extcommunity-list expanded** *listname* **default ip extcommunity-list expanded** *listname* Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.

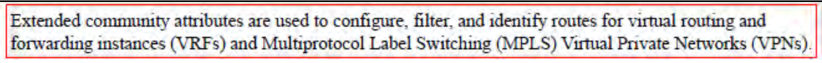
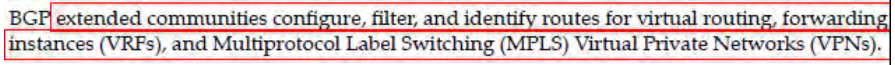
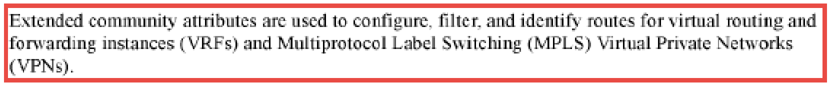
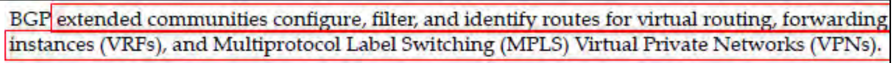
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Route Target Extended Community Attribute** The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites. **Site of Origin Extended Community Attribute** The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Cisco IOS IP Routing: BGP Command Reference (2013), at 330.	 **ip extcommunity-list expanded** The **ip extcommunity-list expanded** command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list. • Route Target (**rt**) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • Site of Origin (**soo**) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.

Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 **Route Target Extended Community Attribute** The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites. **Site of Origin Extended Community Attribute** The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 118.	 **ip extcommunity-list expanded** The **ip extcommunity-list expanded** command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list. • Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.

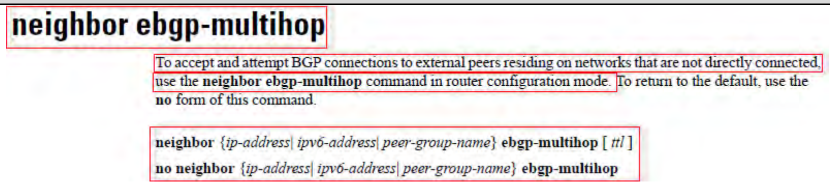
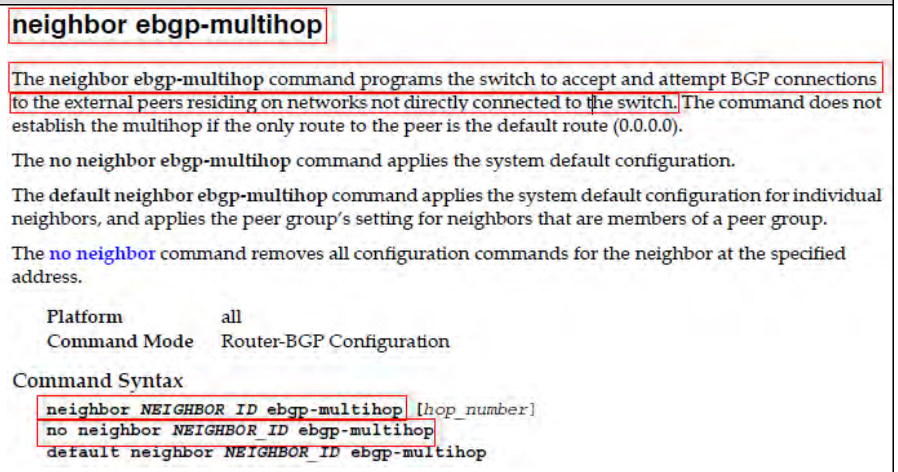
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Route Target Extended Community Attribute** The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites. **Site of Origin Extended Community Attribute** The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Cisco IOS IP Routing: BGP Command Reference (2013), at 330.	 **ip extcommunity-list standard** The **ip extcommunity-list standard** command creates an extended community list to configure Virtua Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). • Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagge with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) route learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1591. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1541; Arista User Manual v. 4.12.3 (7/17/13), at 1365; Arista User Manual, v. 4.11.1 (1/11/13), at 1111; Arista User Manual v. 4.10.3 (10/22/12), at 923; Arista User Manual v. 4.9.3.2 (5/3/12), at 690; Arista User Manual v. 4.8.2 (11/18/11), at 520.

Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 **Route Target Extended Community Attribute** The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites. **Site of Origin Extended Community Attribute** The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 118.	 **ip extcommunity-list standard** The **ip extcommunity-list standard** command creates an extended community list to configure Virtua Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). • Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagge with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. • Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1591. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1541; Arista User Manual v. 4.12.3 (7/17/13), at 1365; Arista User Manual, v. 4.11.1 (1/11/13), at 1111; Arista User Manual v. 4.10.3 (10/22/12), at 923; Arista User Manual v. 4.9.3.2 (5/3/12), at 690; Arista User Manual v. 4.8.2 (11/18/11), at 520.

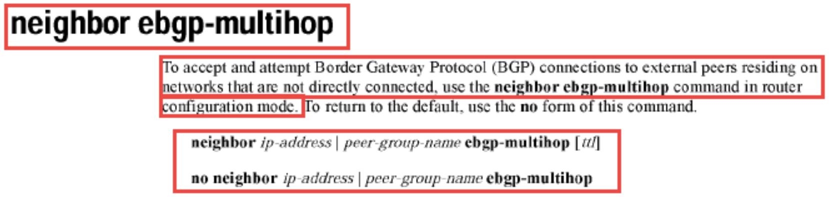
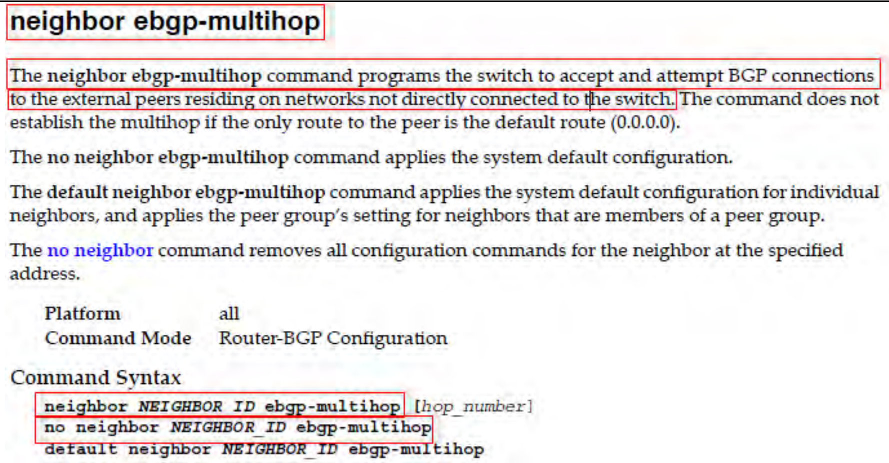
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Route Target Extended Community Attribute** The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites. **Site of Origin Extended Community Attribute** The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Cisco IOS IP Routing: BGP Command Reference (2013), at 330.	 **route targets (rt)**: This attribute identifies a set of sites and VRFs that may receive routes tagged with the configured route target. Configuring this attribute with a route allows that route to be placed in per-site forwarding tables that route traffic received from corresponding sites. **site of origin (soo)**: This attribute identifies the site from where the Provider Edge (PE) router learns the route. All routes learned from a specific site have the same SOO extended community attribute, whether a site is connected to a single or multiple PE routers. This attribute prevents routing loops resulting from multihomed sites. The SOO attribute is configured on the interface and propagated into a BGP domain by redistribution. The SOO is applied to routes learned from VRFs. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1552. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 **Route Target Extended Community Attribute** The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites. **Site of Origin Extended Community Attribute** The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 118.	 **route targets (rt)**: This attribute identifies a set of sites and VRFs that may receive routes tagged with the configured route target. Configuring this attribute with a route allows that route to be placed in per-site forwarding tables that route traffic received from corresponding sites. **site of origin (soo)**: This attribute identifies the site from where the Provider Edge (PE) router learns the route. All routes learned from a specific site have the same SOO extended community attribute, whether a site is connected to a single or multiple PE routers. This attribute prevents routing loops resulting from multihomed sites. The SOO attribute is configured on the interface and propagated into a BGP domain by redistribution. The SOO is applied to routes learned from VRFs. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1552. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.

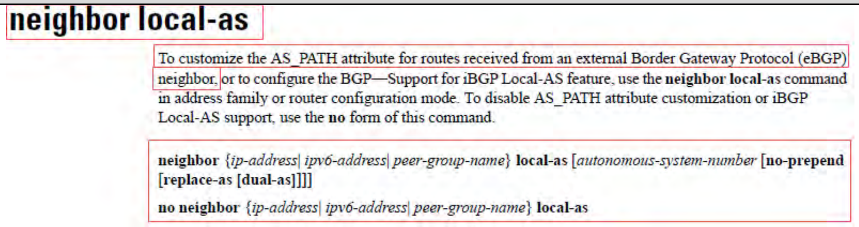
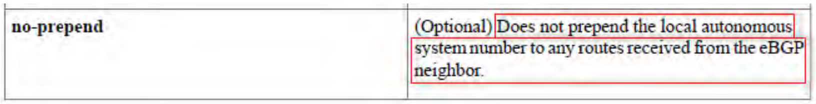
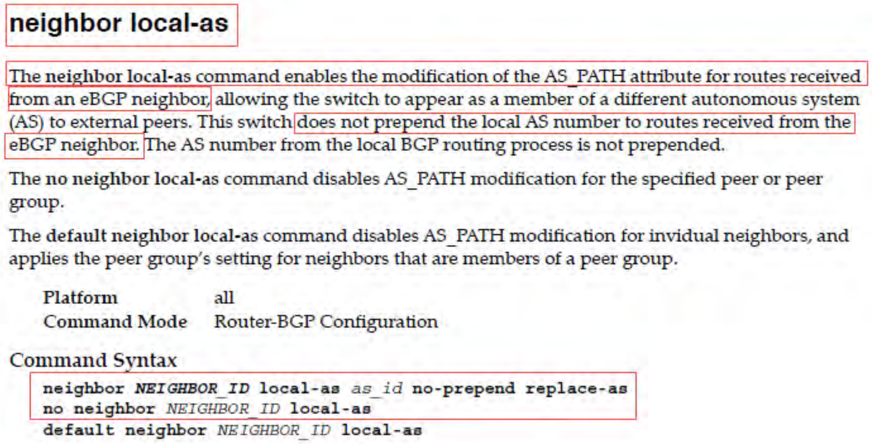
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Cisco IOS IP Routing: BGP Command Reference (2013), at 359	 BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Arista User Manual v. 4.14.3F (Rev. 2) (10/22014), at 1552. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 135.	 BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Arista User Manual v. 4.14.3F (Rev. 2) (10/22014), at 1552. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.

Copyright Registration Information	Cisco	Arista

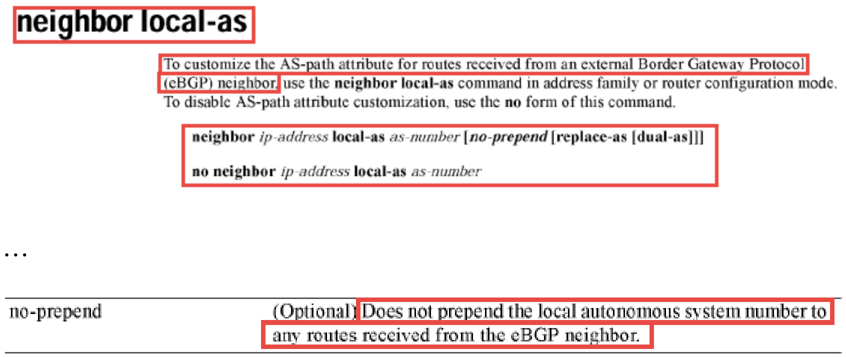
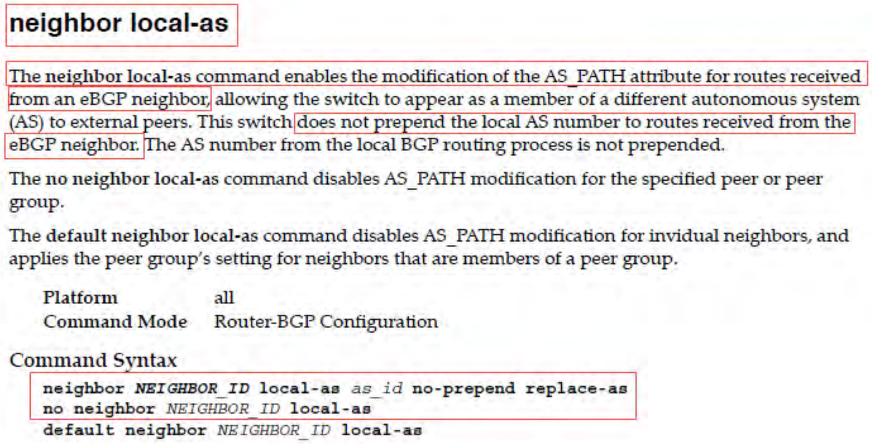
Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	neighbor ebgp-multihop
	To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the **neighbor ebgp-multihop** command in router configuration mode. To return to the default, use the **no** form of this command.
	neighbor {*ip-address*| *ipv6-address*| *peer-group-name*} **ebgp-multihop** [*ttl*]
	no neighbor {*ip-address*| *ipv6-address*| *peer-group-name*} **ebgp-multihop**
	Cisco IOS IP Routing: BGP Command Reference (2013), at 423.
		
		neighbor ebgp-multihop
		The neighbor ebgp-multihop command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0).
		The no neighbor ebgp-multihop command applies the system default configuration.
		The default neighbor ebgp-multihop command applies the system default configuration for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.
		The no neighbor command removes all configuration commands for the neighbor at the specified address.
		Platform all
		Command Mode Router-BGP Configuration
		Command Syntax
		`neighbor NEIGHBOR_ID ebgp-multihop [hop_number]`
		`no neighbor NEIGHBOR_ID ebgp-multihop`
		`default neighbor NEIGHBOR_ID ebgp-multihop`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.

Copyright Registration Information	Cisco	Arista

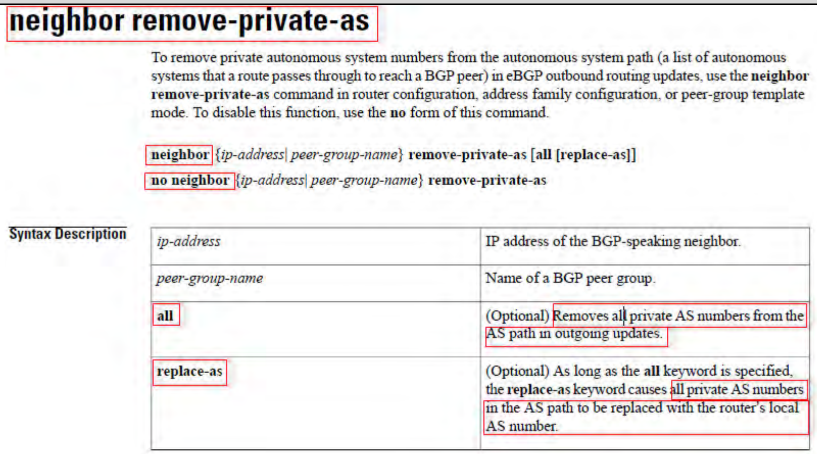
Cisco IOS 12.4
Effective date of registration: 8/12/2005
	
	neighbor ebgp-multihop
	To accept and attempt Border Gateway Protocol (BGP) connections to external peers residing on networks that are not directly connected, use the **neighbor ebgp-multihop** command in router configuration mode. To return to the default, use the **no** form of this command.
	neighbor *ip-address* | *peer-group-name* **ebgp-multihop** [*ttl*]
	no neighbor *ip-address* | *peer-group-name* **ebgp-multihop**
	Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 158.
		
		neighbor ebgp-multihop
		The **neighbor ebgp-multihop** command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0).
		The **no neighbor ebgp-multihop** command applies the system default configuration.
		The **default neighbor ebgp-multihop** command applies the system default configuration for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.
		The **no neighbor** command removes all configuration commands for the neighbor at the specified address.
		Platform all
		Command Mode Router-BGP Configuration
		Command Syntax
		`neighbor NEIGHBOR_ID ebgp-multihop [hop_number]`
		`no neighbor NEIGHBOR_ID ebgp-multihop`
		`default neighbor NEIGHBOR_ID ebgp-multihop`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **neighbor local-as** To customize the AS_PATH attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor, or to configure the BGP—Support for iBGP Local-AS feature, use the **neighbor local-as** command in address family or router configuration mode. To disable AS_PATH attribute customization or iBGP Local-AS support, use the **no** form of this command. **neighbor** {*ip-address*| *ipv6-address*| *peer-group-name*} **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]] **no neighbor** {*ip-address*| *ipv6-address*| *peer-group-name*} **local-as** …  **no-prepend** (Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor. Cisco IOS IP Routing: BGP Command Reference (2013), at 442.	 **neighbor local-as** The **neighbor local-as** command enables the modification of the AS_PATH attribute for routes received from an eBGP neighbor, allowing the switch to appear as a member of a different autonomous system (AS) to external peers. This switch does not prepend the local AS number to routes received from the eBGP neighbor. The AS number from the local BGP routing process is not prepended. The **no neighbor local-as** command disables AS_PATH modification for the specified peer or peer group. The **default neighbor local-as** command disables AS_PATH modification for invidual neighbors, and applies the peer group's setting for neighbors that are members of a peer group. Platform all Command Mode Router-BGP Configuration Command Syntax **neighbor** ***NEIGHBOR_ID*** **local-as** *as_id* **no-prepend replace-as** **no neighbor** *NEIGHBOR_ID* **local-as** **default neighbor** *NEIGHBOR_ID* **local-as** Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1601. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1373; Arista User Manual, v. 4.11.1 (1/11/13), at 1119; Arista User Manual v. 4.10.3 (10/22/12), at 931; Arista User Manual v. 4.9.3.2 (5/3/12), at 696; Arista User Manual v. 4.8.2 (11/18/11), at 526; Arista User Manual v. 4.7.3 (7/18/11), at 386.

Copyright Registration Information	Cisco	Arista

Cisco IOS 12.4
 	
Effective date of registration: 8/12/2005
	
	neighbor local-as
	To customize the AS-path attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor, use the **neighbor local-as** command in address family or router configuration mode. To disable AS-path attribute customization, use the **no** form of this command.
	neighbor *ip-address* **local-as** *as-number* [*no-prepend* [**replace-as** [**dual-as**]]]
	no neighbor *ip-address* **local-as** *as-number*
	…
	no-prepend (Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.
	
	Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 166.
		
		neighbor local-as
		The **neighbor local-as** command enables the modification of the AS_PATH attribute for routes received from an eBGP neighbor, allowing the switch to appear as a member of a different autonomous system (AS) to external peers. This switch does not prepend the local AS number to routes received from the eBGP neighbor. The AS number from the local BGP routing process is not prepended.
		The **no neighbor local-as** command disables AS_PATH modification for the specified peer or peer group.
		The **default neighbor local-as** command disables AS_PATH modification for invidual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.
		Platform all
		Command Mode Router-BGP Configuration
		Command Syntax
		`neighbor NEIGHBOR_ID local-as as_id no-prepend replace-as`
		`no neighbor NEIGHBOR_ID local-as`
		`default neighbor NEIGHBOR_ID local-as`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1601.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1373; Arista User Manual, v. 4.11.1 (1/11/13), at 1119; Arista User Manual v. 4.10.3 (10/22/12), at 931; Arista User Manual v. 4.9.3.2 (5/3/12), at 696; Arista User Manual v. 4.8.2 (11/18/11), at 526; Arista User Manual v. 4.7.3 (7/18/11), at 386.

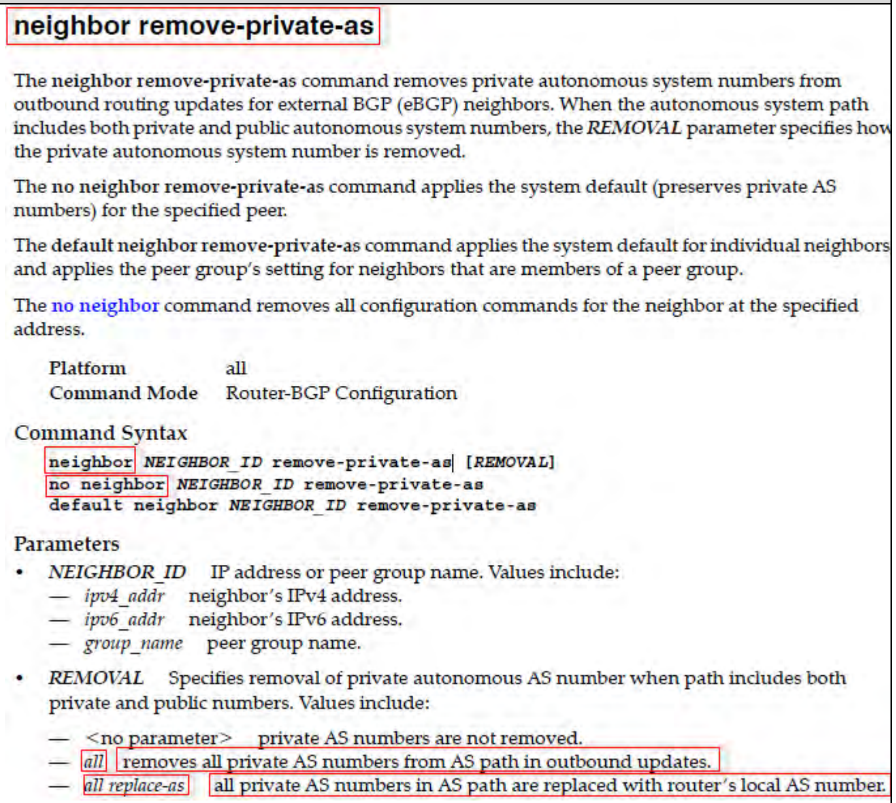
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>
<b>neighbor remove-private-as</b>

To remove private autonomous system numbers from the autonomous system path (a list of autonomous systems that a route passes through to reach a BGP peer) in eBGP outbound routing updates, use the <b>neighbor remove-private-as</b> command in router configuration, address family configuration, or peer-group template mode. To disable this function, use the <b>no</b> form of this command.

<b>neighbor</b> {<i>ip-address</i>| <i>peer-group-name</i>} <b>remove-private-as [all [replace-as]]</b>
<b>no neighbor</b> {<i>ip-address</i>| <i>peer-group-name</i>} <b>remove-private-as</b>

<b>Syntax Description</b>
<table>
<tr><td><i>ip-address</i></td><td>IP address of the BGP-speaking neighbor.</td></tr>
<tr><td><i>peer-group-name</i></td><td>Name of a BGP peer group.</td></tr>
<tr><td><b>all</b></td><td>(Optional) Removes all private AS numbers from the AS path in outgoing updates.</td></tr>
<tr><td><b>replace-as</b></td><td>(Optional) As long as the <b>all</b> keyword is specified, the <b>replace-as</b> keyword causes all private AS numbers in the AS path to be replaced with the router's local AS number.</td></tr>
</table>

Cisco IOS IP Routing: BGP Command Reference (2013), at 479.</td>
<td>
<b>neighbor remove-private-as</b>

The <b>neighbor remove-private-as</b> command removes private autonomous system numbers from outbound routing updates for external BGP (eBGP) neighbors. When the autonomous system path includes both private and public autonomous system numbers, the <i>REMOVAL</i> parameter specifies how the private autonomous system number is removed.

The <b>no neighbor remove-private-as</b> command applies the system default (preserves private AS numbers) for the specified peer.

The <b>default neighbor remove-private-as</b> command applies the system default for individual neighbors and applies the peer group's setting for neighbors that are members of a peer group.

The no neighbor command removes all configuration commands for the neighbor at the specified address.

<b>Platform</b> all
<b>Command Mode</b> Router-BGP Configuration

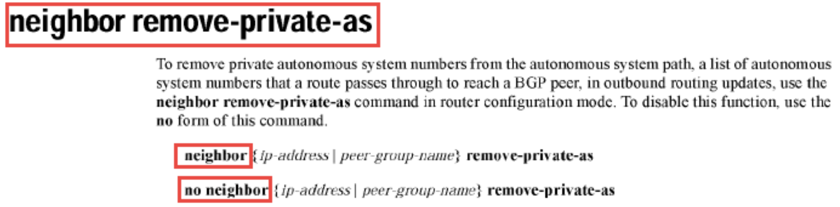
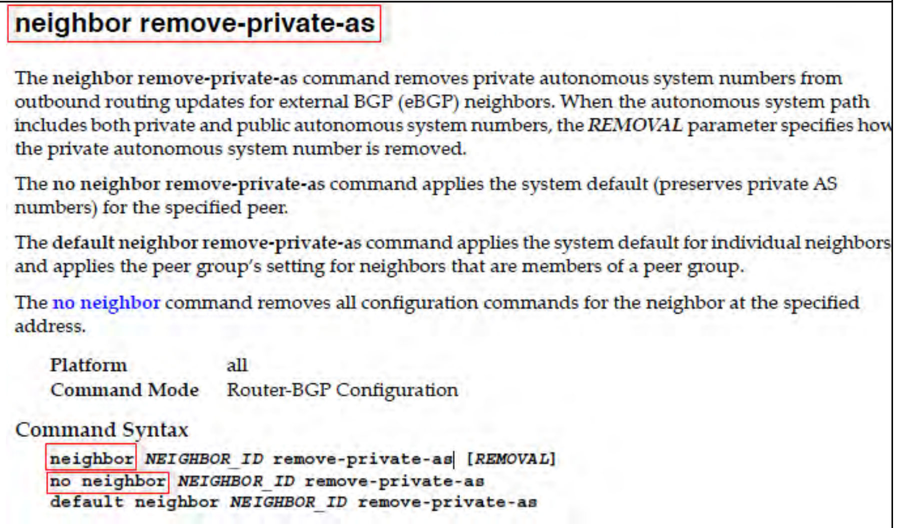
Command Syntax
<code>neighbor <i>NEIGHBOR_ID</i> remove-private-as [<i>REMOVAL</i>]</code>
<code>no neighbor <i>NEIGHBOR_ID</i> remove-private-as</code>
<code>default neighbor <i>NEIGHBOR_ID</i> remove-private-as</code>

Parameters
• <i>NEIGHBOR_ID</i> IP address or peer group name. Values include:
— <i>ipv4_addr</i> neighbor's IPv4 address.
— <i>ipv6_addr</i> neighbor's IPv6 address.
— <i>group_name</i> peer group name.
• <i>REMOVAL</i> Specifies removal of private autonomous AS number when path includes both private and public numbers. Values include:
— &lt;no parameter&gt; private AS numbers are not removed.
— <i>all</i> removes all private AS numbers from AS path in outbound updates.
— <i>all replace-as</i> all private AS numbers in AS path are replaced with router's local AS number.

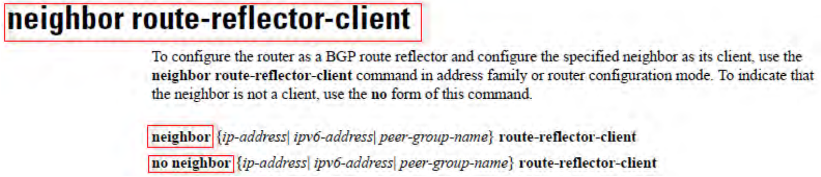
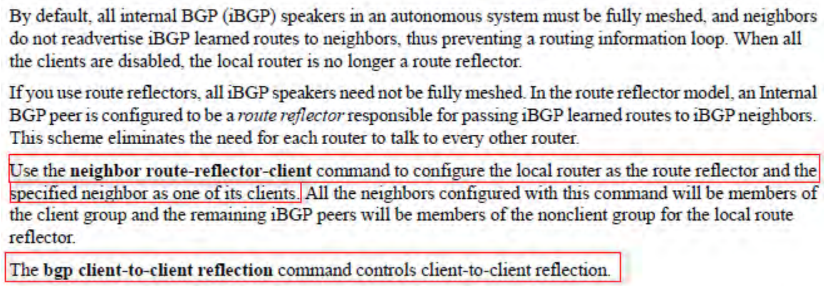
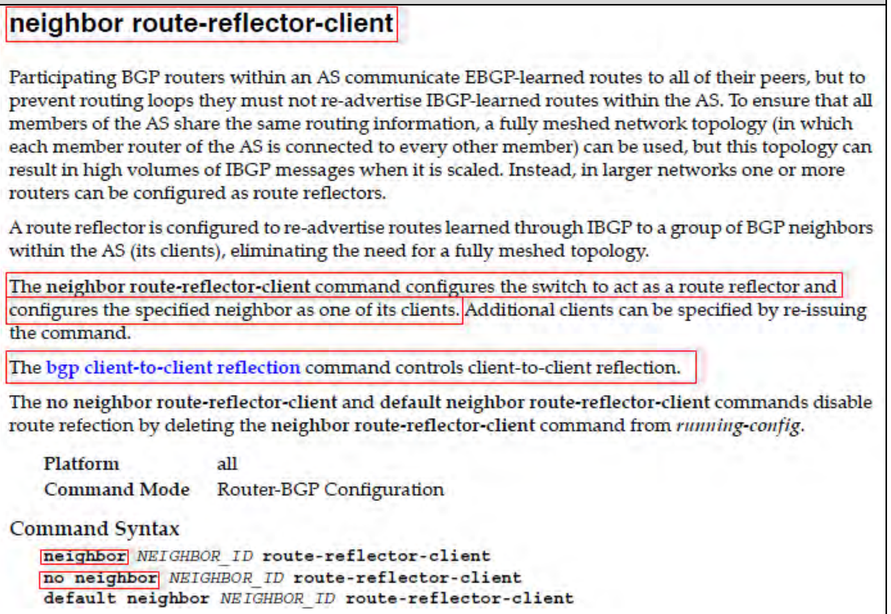
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1612.

<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1384; Arista User Manual, v. 4.11.1 (1/11/13), at 1130.</td>
</tr>
</table>

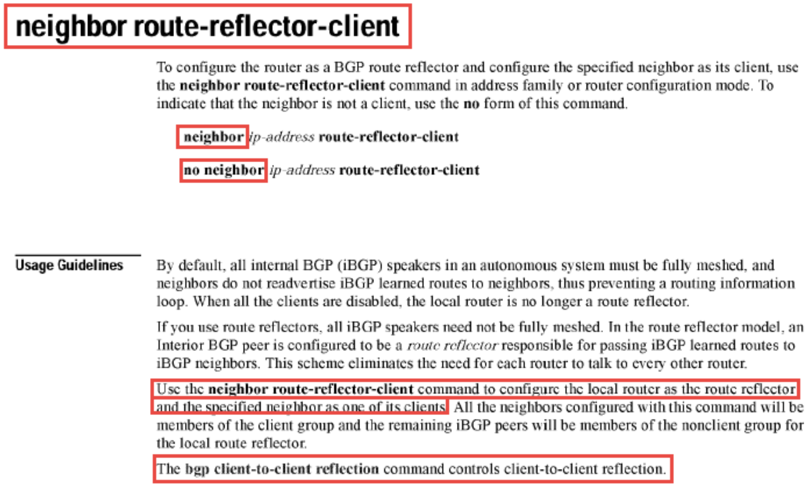
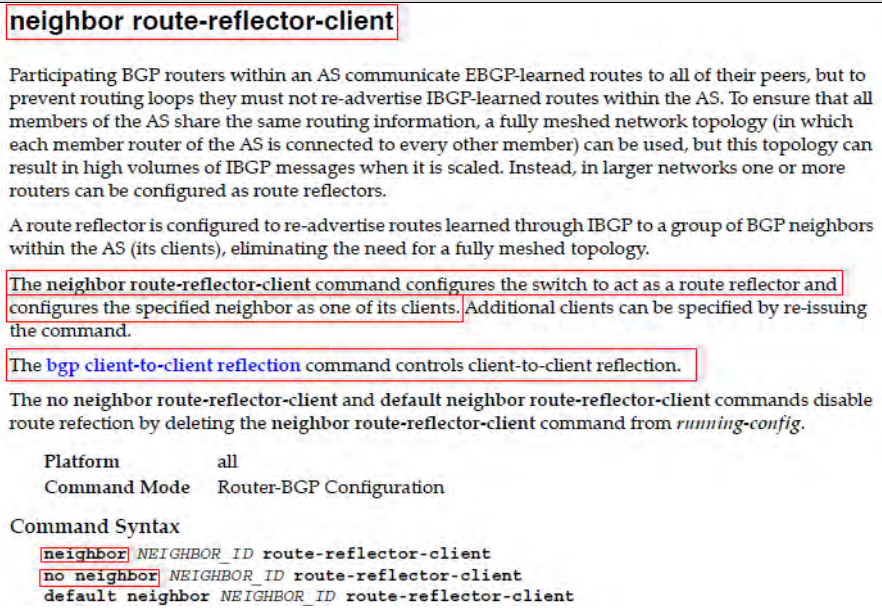
Copyright Registration Information	Cisco	Arista

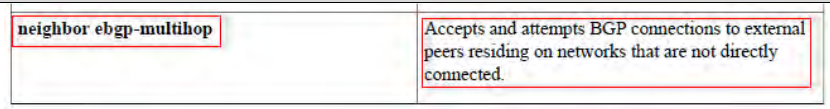
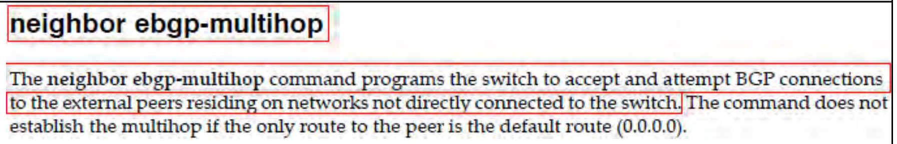
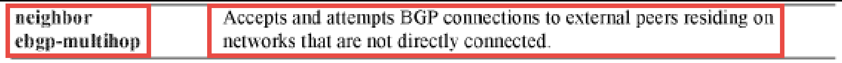
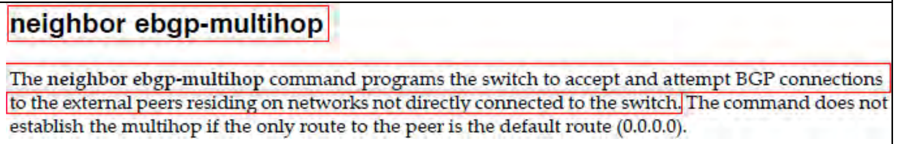
Cisco IOS 12.4
Effective date of registration: 8/12/2005
	
	neighbor remove-private-as
	To remove private autonomous system numbers from the autonomous system path, a list of autonomous system numbers that a route passes through to reach a BGP peer, in outbound routing updates, use the **neighbor remove-private-as** command in router configuration mode. To disable this function, use the **no** form of this command.
	neighbor {*ip-address* | *peer-group-name*} **remove-private-as**
	no neighbor {*ip-address* | *peer-group-name*} **remove-private-as**
	Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 188.
		
		neighbor remove-private-as
		The **neighbor remove-private-as** command removes private autonomous system numbers from outbound routing updates for external BGP (eBGP) neighbors. When the autonomous system path includes both private and public autonomous system numbers, the *REMOVAL* parameter specifies how the private autonomous system number is removed.
		The **no neighbor remove-private-as** command applies the system default (preserves private AS numbers) for the specified peer.
		The **default neighbor remove-private-as** command applies the system default for individual neighbors and applies the peer group's setting for neighbors that are members of a peer group.
		The **no neighbor** command removes all configuration commands for the neighbor at the specified address.
		Platform all
		Command Mode Router-BGP Configuration
		Command Syntax
		`neighbor NEIGHBOR_ID remove-private-as [REMOVAL]`
		`no neighbor NEIGHBOR_ID remove-private-as`
		`default neighbor NEIGHBOR_ID remove-private-as`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1612.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1384; Arista User Manual, v. 4.11.1 (1/11/13), at 1130.

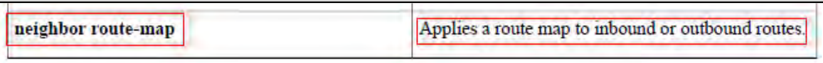
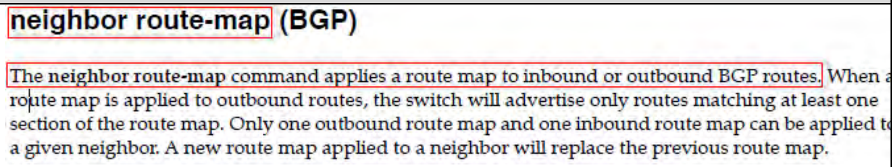
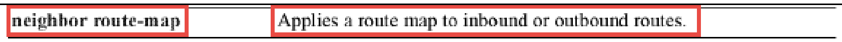
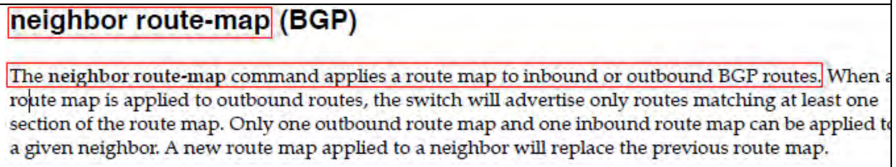
Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	neighbor route-reflector-client
	To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the **neighbor route-reflector-client** command in address family or router configuration mode. To indicate that the neighbor is not a client, use the **no** form of this command.
	neighbor {*ip-address*| *ipv6-address*| *peer-group-name*} **route-reflector-client**
	no neighbor {*ip-address*| *ipv6-address*| *peer-group-name*} **route-reflector-client**
	Cisco IOS IP Routing: BGP Command Reference (2013), at 486
	
	By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.
	If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Internal BGP peer is configured to be a *route reflector* responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.
	Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.
	The **bgp client-to-client reflection** command controls client-to-client reflection.
	Cisco IOS IP Routing: BGP Command Reference (2013), at 487.
		
		neighbor route-reflector-client
		Participating BGP routers within an AS communicate EBGP-learned routes to all of their peers, but to prevent routing loops they must not re-advertise IBGP-learned routes within the AS. To ensure that all members of the AS share the same routing information, a fully meshed network topology (in which each member router of the AS is connected to every other member) can be used, but this topology can result in high volumes of IBGP messages when it is scaled. Instead, in larger networks one or more routers can be configured as route reflectors.
		A route reflector is configured to re-advertise routes learned through IBGP to a group of BGP neighbors within the AS (its clients), eliminating the need for a fully meshed topology.
		The **neighbor route-reflector-client** command configures the switch to act as a route reflector and configures the specified neighbor as one of its clients. Additional clients can be specified by re-issuing the command.
		The **bgp client-to-client reflection** command controls client-to-client reflection.
		The **no neighbor route-reflector-client** and **default neighbor route-reflector-client** commands disable route refection by deleting the **neighbor route-reflector-client** command from *running-config*.
		Platform all
		Command Mode Router-BGP Configuration
		Command Syntax
		`neighbor NEIGHBOR_ID route-reflector-client`
		`no neighbor NEIGHBOR_ID route-reflector-client`
		`default neighbor NEIGHBOR_ID route-reflector-client`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1614.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1386; Arista User Manual, v. 4.11.1 (1/11/13), at 1132.

Copyright Registration Information	Cisco	Arista

Cisco IOS 12.4
 	
Effective date of registration: 8/12/2005
	
	neighbor route-reflector-client
	To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the **neighbor route-reflector-client** command in address family or router configuration mode. To indicate that the neighbor is not a client, use the **no** form of this command.
	neighbor *ip-address* **route-reflector-client**
	no neighbor *ip-address* **route-reflector-client**
	Usage Guidelines
	By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.
	If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a *route reflector* responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.
	Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.
	The **bgp client-to-client reflection** command controls client-to-client reflection.
	
	Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 192.
		
		neighbor route-reflector-client
		Participating BGP routers within an AS communicate EBGP-learned routes to all of their peers, but to prevent routing loops they must not re-advertise IBGP-learned routes within the AS. To ensure that all members of the AS share the same routing information, a fully meshed network topology (in which each member router of the AS is connected to every other member) can be used, but this topology can result in high volumes of IBGP messages when it is scaled. Instead, in larger networks one or more routers can be configured as route reflectors.
		A route reflector is configured to re-advertise routes learned through IBGP to a group of BGP neighbors within the AS (its clients), eliminating the need for a fully meshed topology.
		The **neighbor route-reflector-client** command configures the switch to act as a route reflector and configures the specified neighbor as one of its clients. Additional clients can be specified by re-issuing the command.
		The bgp client-to-client reflection command controls client-to-client reflection.
		The **no neighbor route-reflector-client** and **default neighbor route-reflector-client** commands disable route refection by deleting the **neighbor route-reflector-client** command from *running-config*.
		Platform all
		Command Mode Router-BGP Configuration
		Command Syntax
		`neighbor NEIGHBOR_ID route-reflector-client`
		`no neighbor NEIGHBOR_ID route-reflector-client`
		`default neighbor NEIGHBOR_ID route-reflector-client`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1614.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1386; Arista User Manual, v. 4.11.1 (1/11/13), at 1132.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **neighbor ebgp-multihop** Accepts and attempts BGP connections to external peers residing on networks that are not directly connected. Cisco IOS IP Routing: BGP Command Reference (2013), at 416.	 **neighbor ebgp-multihop** The neighbor ebgp-multihop command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0). Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 **neighbor ebgp-multihop** Accepts and attempts BGP connections to external peers residing on networks that are not directly connected. Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 173.	 **neighbor ebgp-multihop** The neighbor ebgp-multihop command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0). Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 neighbor route-map Applies a route map to inbound or outbound routes. Cisco IOS IP Routing: BGP Command Reference (2013), at 524.	 **neighbor route-map (BGP)** The **neighbor route-map** command applies a route map to inbound or outbound BGP routes. When a route map is applied to outbound routes, the switch will advertise only routes matching at least one section of the route map. Only one outbound route map and one inbound route map can be applied to a given neighbor. A new route map applied to a neighbor will replace the previous route map. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1613. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1385; Arista User Manual, v. 4.11.1 (1/11/13), at 1131; Arista User Manual v. 4.10.3 (10/22/12), at 943.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 neighbor route-map Applies a route map to inbound or outbound routes. Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 204.	 **neighbor route-map (BGP)** The **neighbor route-map** command applies a route map to inbound or outbound BGP routes. When a route map is applied to outbound routes, the switch will advertise only routes matching at least one section of the route map. Only one outbound route map and one inbound route map can be applied to a given neighbor. A new route map applied to a neighbor will replace the previous route map. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1613. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1385; Arista User Manual, v. 4.11.1 (1/11/13), at 1131; Arista User Manual v. 4.10.3 (10/22/12), at 943.